UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/730,641	12/05/2000	Ching-Chih (Jason) Han	CREO.009US0	9293

25242 7590 04/22/2005

VICTOR H. OKUMOTO
P.O. BOX 6120
FREMONT, CA 94538

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No. 09/730,641	Applicant(s) HAN ET AL.	
	Examiner Courtney D. Fields	Art Unit 2137	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 24 March 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: *The word "licensee" which replaces the word "recipient" changes the scope of the invention*. (See 37 CFR 1.116 and 41.33(a)).
4. ☒ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Notice of Non-Compliant Amendment (37 CFR 1.121)	Application No.	Applicant(s)	
	09/730,641	HAN ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

The amendment document filed on *24 March 2005* is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121. In order for the amendment document to be compliant, correction of the following item(s) is required.

THE FOLLOWING MARKED (X) ITEM(S) CAUSE THE AMENDMENT DOCUMENT TO BE NON-COMPLIANT:

- ☐ 1. Amendments to the specification:
  - ☐ A. Amended paragraph(s) do not include markings.
  - ☐ B. New paragraph(s) should not be underlined.
  - ☐ C. Other _____.
- ☐ 2. Abstract:
  - ☐ A. Not presented on a separate sheet. 37 CFR 1.72.
  - ☐ B. Other _____.
- ☐ 3. Amendments to the drawings:
  - ☐ A. The drawings are not properly identified in the top margin as "Replacement Sheet," "New Sheet," or "Annotated Sheet" as required by 37 CFR 1.121(d).
  - ☐ B. The practice of submitting proposed drawing correction has been eliminated. Replacement drawings showing amended figures, without markings, in compliance with 37 CFR 1.84 are required.
  - ☐ C. Other _____.
- ☒ 4. Amendments to the claims:
  - ☐ A. A complete listing of all of the claims is not present.
  - ☐ B. The listing of claims does not include the text of all pending claims (including withdrawn claims)
  - ☐ C. Each claim has not been provided with the proper status identifier, and as such, the individual status of each claim cannot be identified. Note: the status of every claim must be indicated after its claim number by using one of the following status identifiers: (Original), (Currently amended), (Canceled), (Previously presented), (New), (Not entered), (Withdrawn) and (Withdrawn-currently amended).
  - ☐ D. The claims of this amendment paper have not been presented in ascending numerical order.
  - ☒ E. Other: *The claims have been amended, however, the Applicant failed to identify changes by using strikethrough or double brackets to show deleted text.*

For further explanation of the amendment format required by 37 CFR 1.121, see MPEP § 714 and the USPTO website at http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/officeflyer.pdf .

TIME PERIODS FOR FILING A REPLY TO THIS NOTICE:

1. Applicant is given **no new time period** if the non-compliant amendment is an after-final amendment or an amendment filed after allowance. If applicant wishes to resubmit the non-compliant after-final amendment with corrections, the **entire corrected amendment** must be resubmitted within the time period set forth in the final Office action.

2. Applicant is given **one month**, or thirty (30) days, whichever is longer, from the mail date of this notice to supply the **corrected section** of the non-compliant amendment in compliance with 37 CFR 1.121, if the non-compliant amendment is one of the following: a preliminary amendment, a non-final amendment (including a submission for a request for continued examination (RCE) under 37 CFR 1.114), a supplemental amendment filed within a suspension period under 37 CFR 1.103(a) or (c), and an amendment filed in response to a *Quayle* action.

   Extensions of time are available under 37 CFR 1.136(a) only if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action.

   Failure to timely respond to this notice will result in:
   Abandonment of the application if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action; or
   Non-entry of the amendment if the non-compliant amendment is a preliminary amendment or supplemental amendment.

5

Escrowed Encryption and Related Issues

This chapter describes a tool--escrowed encryption--that responds to the needs described in Chapter 3 for exceptional access to encrypted information. Escrowed encryption is the basis for a number of Administration proposals that seek to reconcile needs for information security against the needs of law enforcement and to a lesser extent national security. As in the case of export controls, escrowed encryption generates considerable controversy.

5.1 WHAT IS ESCROWED ENCRYPTION?

The term "escrow," as used conventionally, implies that some item of value (e.g., a trust deed, money, real property, other physical object) is delivered to an independent trusted party that might be a person or an organization (i.e., an escrow agent) for safekeeping, and is accompanied by a set of rules provided by the parties involved in the transaction governing the actions of the escrow agent. Such rules typically specify what is to be done with the item, the schedule to be followed, and the list of other events that have to occur. The underlying notion is that the escrow agent is a secure haven for temporary ownership or possession of the item, is legally bound to comply with the set of rules for its disposition, functions as a disinterested extratransaction party, and bears legal liability for malfeasance or mistakes.

Usually, the rules stipulate that when all conditions set forth in the escrow rules have been fulfilled, the item will eventually be delivered to a specified party (e.g., possibly the original depositing party, an estate, a judicial officer for custody, one or more individuals or organizations). In any event, the salient point is that all terms and conditions and functioning of an escrow process are, or can be, visible to the parties involved; moreover, the behavior and performance of formal escrow agents are governed by legally established obligations.

As it applies to cryptography, the term "escrow" was introduced by the U.S. government's April 1993 Clipper initiative in the context of encryption keys. Prior to this time, the term "escrow" had not been widely associated with cryptography, although the underlying concepts had been

known for some time (as described below). The Clipper initiative promoting escrowed encryption was intended "to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement."1 In this original context, the term "escrowed encryption" had a very specific and narrow meaning: escrowed encryption was a mechanism that would assure law enforcement access to the voice communications underlying encrypted intercepts from wiretaps.

However, during 3 years of public debate and dialogue, "escrow," "key escrow," and "escrowed encryption" have become terms with a much broader meaning. Indeed, many different schemes for "escrowed encryption" are quite different from "escrowed encryption" as the term was used in the Clipper initiative.

As is so often the case in computer-related matters, terminology for escrowed systems is today not clearly established and can be confusing or misleading. While new terminology could be introduced in an effort to clarify meaning, the fact is that the present policy and public and technical dialogues all use "escrow" and "escrowed encryption" in a very generic and broad sense. It is no longer the very precise restricted concept embodied in the Clipper initiative and described in Section 5.2.1. Escrow as a concept now applies not only to the initial purpose of assuring law enforcement access to encrypted materials, but also to possible end-user or organizational requirements for a mechanism to protect against lost, corrupted, or unavailable keys. It can also mean that some process such as authority to decrypt a header containing a session key is escrowed with a trusted party, or it can mean that a corporation is ready to cooperate with law enforcement to access encrypted materials.

This report conforms to current usage, considering escrowed encryption as a broad concept that can be implemented in many ways; Section 5.3 addresses forms of escrowed encryption other than that described in the Clipper initiative. Also, escrowed encryption is only one of several approaches to providing exceptional access to encrypted information; nonescrow approaches to providing exceptional access are discussed in Chapter 7.2

Finally, the relationship between "strong encryption" and "escrowed encryption" should be noted. As stated above, escrowed encryption refers to an approach to encryption that

enables exceptional access to plaintext without requiring a third party (e.g., government acting with legal authorization, a corporation acting in accordance with its contractual rights vis-ˆ-vis its employees, an individual who has lost an encryption key) to perform a cryptanalytic attack. At the same time, escrowed encryption can involve cryptographic algorithms that are strong or weak and keys that are long or short. Some participants in the public debate appear to believe that escrowed encryption is necessarily equivalent to weak encryption, because it does not prevent third parties from having access to the relevant plaintext. But this is a mischaracterization of the intent behind escrowed encryption, since all escrowed encryption schemes proposed to date are intended to provide very strong cryptographic confidentiality (strong algorithms, relatively long keys) for users against unauthorized third parties, but no confidentiality at all against third parties who have authorized exceptional access.

5.2 ADMINISTRATION INITIATIVES SUPPORTING ESCROWED ENCRYPTION

Since inheriting the problem of providing law enforcement access to encrypted telephony from the outgoing Bush Administration in late 1992, Clinton Administration officials have said that as they considered the not-so-distant future of information technology and information security along with the stated needs of law enforcement and national security for access to information, they saw three alternatives:3

- To do nothing, resulting in the possible proliferation of products with encryption capabilities that would seriously weaken, if not wholly negate, the authority to wiretap embodied in the Wiretap Act of 1968 (Title III) and damage intelligence collection for national security and foreign policy reasons;
- To support an approach based on weak encryption, likely resulting in poor security and cryptographic confidentiality for important personal and business information; and
- To support an approach based on strong but escrowed encryption. If widely adopted and properly implemented, escrowed encryption could provide legitimate users with high degrees of assurance that their sensitive information would remain secure but nevertheless enable law enforcement and national security authorities to obtain access to escrow-encrypted data in specific instances when authorized under law. Moreover, the Administration hoped that by meeting

legitimate demands for better information security, escrowed encryption would dampen the market for unescrowed encryption products that would deny access to law enforcement and national security authorities even when they sought access for legitimate and lawfully authorized purposes.

The Administration chose the last, and since April 1993, the U.S. government has advanced a number of initiatives to support the insertion of key escrow features into products with encryption capabilities that will become available in the future. These include the Clipper initiative and the Escrowed Encryption Standard, the Capstone/Fortezza initiative, and the proposal to liberalize export controls on products using escrowed encryption. These initiatives raise a number of important issues that are the focus of Sections 5.3 to 5.13.

5.2.1 The Clipper Initiative and the Escrowed Encryption Standard

As noted above, the Clipper initiative was conceived as a way for providing legal access by law enforcement authorities to encrypted telephony.4 The Escrowed Encryption Standard (EES; a Federal Information Processing Standard, FIPS-185) was promulgated in February 1994 as the key technological component of the Clipper initiative (Box 5.1). Specifically, the EES called for the integration of special microelectronic integrated circuit chips (called "Clipper chips") into devices used for voice communications; these chips, as one part of an overall system, provide voice confidentiality for the user and exceptional access to law enforcement authorities. To provide these functions, the Clipper chip was designed with a number of essential characteristics:

Box 5.1
Key Technical Attributes of the Clipper Initiative

1. A chip-unique secret key--the "unit key" or "device key" or "master key"--would be embedded in the chip at the time of fabrication and could be obtained by law enforcement officials legally authorized to do so under Title III.
2. Each chip-unique device key would be split into two components.
3. The component parts would be deposited with and held under high security by two trusted third-party escrow agents proposed to be agencies of the U.S. government. Note:

"Third-party" is used here to indicate parties other than those participating in the communication.
4. A law enforcement access field (LEAF) would be a required part of every transmission. The LEAF would contain (a) the current session key, encrypted with a combination of the device-unique master key and a different but secret "family key" also permanently embedded in the chip, and (b) the chip serial number, also protected by encryption with the family key.
5. Law enforcement could use the information in the LEAF to identify the particular device of interest, solicit its master-key components from the two escrow agents, combine them, recover the session key, and eventually decrypt the encrypted traffic.
6. The encryption algorithm on the chip would be secret.
7. The chip would be protected against reverse engineering and other attempts to access its technical details.

SOURCE: Dorothy Denning and Miles Smid, "Key Escrowing Today," IEEE Communications, Volume 32(9), September 1994, pp. 58-68. Available on-line at http://www.cosc.georgetown.edu/~denning/ crypto/Key-Escrowing-Today.txt.

• Confidentiality would be provided by a classified algorithm known as Skipjack. Using an 80-bit key, the Skipjack algorithm would offer considerably more protection against brute-force attacks than the 56-bit DES algorithm (FIPS 46-1). The Skipjack algorithm was reviewed by several independent experts, all with the necessary security clearances. In the course of an investigation limited by time and resources, they reported that they did not find shortcuts that would significantly reduce the time to perform a cryptanalytic attack below what would be required by brute force.5
• The chip would be protected against reverse engineering and other attempts to access its technical details.
• The chip would be factory-programmed with a chip-unique secret key, the "unit key" or "device key,"6 at the time of fabrication. Possession of this key would enable one to decrypt all communications sent to and from the telephone unit in which the chip was integrated.
• A law enforcement access field (LEAF) would be a required part of every transmission and would be generated by the chip. The LEAF would contain two items: (a) the current session key,7 encrypted with a combination of the device-unique unit key, and (b) the chip serial number. The entire LEAF would itself be encrypted by a different but secret

"family key" also permanently embedded in the chip. The family key would be the same in all Clipper chips produced by a given manufacturer; in practice, all Clipper chips regardless of manufacturer are programmed today by the Mykotronx Corporation with the same family key.

To manage the use of the LEAF, the U.S. government would undertake a number of actions:

• The unit key, known at the time of manufacture and unchangeable for the life of the chip, would be divided into two components, each of which would be deposited with and held under high security by two trusted government escrow agents located within the Departments of Commerce and Treasury.
• These escrow agents would serve as repositories for all such materials, releasing the relevant information to law enforcement authorities upon presentation of the unit identification and lawfully obtained court orders.
When law enforcement officials encountered a Clipper-encrypted conversation on a wiretap, they would use the LEAF to obtain the serial number of the Clipper chip performing the encryption and the encrypted session key.8 Upon presentation of the serial number and court authorization for the wiretap to the escrow agents, law enforcement officials could then obtain the proper unit-key components, combine them, recover the session key, and eventually decrypt the encrypted voice communications.9 Only one key would be required in order to obtain access to both sides of the Clipper-encrypted conversation. The authority for law enforcement to approach escrow agents and request unit-key components was considered to be that granted by Title III and the Foreign Intelligence Surveillance Act (FISA).10

As a FIPS, the EES is intended for use by the federal government and has no legal standing outside the federal government. Indeed, its use is optional even by federal agencies. In other words, federal agencies with a requirement for secure voice communications have a choice about whether or not to adopt the EES for their own purposes. More importantly, the use of EES-compliant devices by private parties cannot in general be compelled by executive action alone; private consumers are free to decide whether or not to use EES-compliant devices to safeguard communications and are free to use other approaches to communications security should they so desire.11 However, if consumers choose to use EES-compliant devices, they must accept key escrow as outlined in procedures promulgated by

the government. This characteristic--that interoperability requires acceptance of key escrow--is a design choice; a different specification could permit the interoperability of devices with or without features for key escrow.

The EES was developed by communications security experts from the NSA, but the escrow features of the EES are intended to meet the needs of law enforcement--i.e., its needs for clandestine surveillance of electronic and wire communications as described in Chapter 3. NSA played this development role because of its technical expertise. EES-compliant devices are also approved for communicating classified information up to and including SECRET. In speaking with the committee, Administration officials described the Clipper initiative as more or less irrelevant to the needs of signals intelligence (SIGINT) (Box 5.2).

Box 5.2
The Relationship of Escrowed Encryption to Signals Intelligence

Escrowed encryption--especially the Escrowed Encryption Standard (EES) and the Clipper initiative--is a tool of law enforcement more than of signals intelligence (SIGINT). The EES was intended primarily for domestic use, although exports of EES-compliant devices have not been particularly discouraged. Given that the exceptional access feature of escrowed encryption has been openly announced, purchase by foreign governments for secure communications is highly unlikely.

On the other hand, the U.S. government has classified the Skipjack algorithm to keep foreign adversaries from learning more about good cryptography. In addition, wide deployment and use of escrowed encryption would complicate the task of signals intelligence, simply because individual keys would have to be obtained one by one for communications that might or might not be useful. (Still, EES devices would be better for SIGINT than unescrowed secure telephones, in the sense that widely deployed secure telephones without features for exceptional access would be much harder to penetrate.)

Finally, the impact of escrowed encryption on intelligence collection abroad depends on the specific terms of escrow agent certification. Even assuming that all relevant escrow agents are located within the United States (a question addressed at greater length in Appendix G), the specific

regulations governing their behavior are relevant. Intelligence collections of digital data can proceed with few difficulties if regulations permit escrow agents to make keys available to national security authorities on an automated basis and without the need to request keys one by one. On the other hand, if the regulations forbid wholesale access to keys (and the products in question do not include a "universal key" that allows one key to decrypt messages produced by many devices), escrowed encryption would provide access primarily to specific encrypted communications that are known to be intrinsically interesting (e.g., known to be from a particular party of interest). However, escrowed encryption without wholesale access to keys would not provide significant assistance to intelligence collections undertaken on a large scale.

As of early 1996, AT&T had sold 10,000 to 15,000 units of the Surity Telephone Device 3600. These include four configurations: Model C, containing only the Clipper chip, which has been purchased primarily by U.S. government customers; Model F, containing only an AT&T-proprietary algorithm that is exportable; Model P, containing an AT&T-proprietary nonexportable algorithm in addition to the exportable algorithm; and Model S, with all three of the above. Only units with the Clipper chip have a key-escrow feature. All the telephones are interoperable--they negotiate with each other to settle on a mutually available algorithm at the beginning of a call.12 In addition, AT&T and Cycomm International have agreed to jointly develop and market Clipper-compatible digital voice encryption attachments for Motorola's Micro-Tac series of handheld cellular telephones; these products are expected to be available in the second quarter of 1996.13 Finally, AT&T makes no particular secret of the fact that its Surity line of secure voice communication products employs Clipper chip technology, but that fact is not featured in the product literature; potential consumers would have to know enough to ask a knowledgeable sales representative.

5.2.2 The Capstone/Fortezza Initiative14

The Capstone/Fortezza effort supports escrowed encryption for data storage and communications, although a FIPS for this application has not been issued. Specifically, the Capstone chip is an integrated-circuit chip that provides a number of encryption services for both stored computer data and data communications. For confidentiality, the Capstone

chip uses the Skipjack algorithm, the same algorithm that is used in the Clipper chip (which is intended only for voice communications, including low-speed data and fax transmission across the public switched telephone network, and the same mechanism to provide for key escrowing. The agents used to hold Capstone keys are also identical to those for holding Clipper keys--namely, the Departments of Treasury and Commerce. In addition, the Capstone chip (in contrast to the Clipper chip) provides services that conform to the Digital Signature Standard (FIPS-186) to provide digital signatures that authenticate user identity and the Secure Hash Standard (FIPS-180); the chip also implements a classified algorithm for key exchange (usually referred to as the Key Exchange Algorithm (KEA)) and a random number generator.

The Capstone chip is the heart of the Fortezza card.15 The Fortezza card is a PC-card (formerly known as a PCMCIA card) intended to be plugged into any computer with a PC-card expansion slot and appropriate support software; with the card in place, the host computer is able to provide reliable user authentication and encryption for confidentiality and certify data transmission integrity in any communication with any other computer so equipped. The Fortezza card is an example of a hardware token that can be used to ensure proper authentication.16 Note also that there are other hardware PC cards that provide cryptographic functionality similar to that of Fortezza but without the escrow features.17

To date, the NSA has issued two major solicitations for Fortezza cards, the second of which was for 750,000 cards.18 These cards will be used by those on the Defense Messaging System, a communications network that is expected to accommodate up to 2 million Defense Department users in 2005. In addition, Fortezza cards are intended to be available for private sector use. The extent to which Fortezza cards will be acceptable in the commercial market remains to be seen, although a number of product vendors have decided to incorporate support for Fortezza cards in some products.19

5.2.3 The Relaxation of Export Controls on Software Products Using "Properly Escrowed" 64-bit Encryption

As noted in Chapter 4, the Administration has proposed to treat software products using a 64-bit encryption key as it currently treats products with encryption capabilities that

are based on a 40-bit RC2 or RC4 algorithm, providing that products using this stronger encryption are "properly escrowed." This change is intended to facilitate the global sale of U.S. software products with significantly stronger cryptographic protection than is available from U.S. products sold abroad today.

To work out the details of what is meant by "properly escrowed," the National Institute of Standards and Technology held workshops in September and December 1995 at which the Administration released a number of draft criteria for export control (Box 5.3). These criteria are intended to ensure that a product's key escrow mechanism cannot be readily altered or bypassed so as to defeat the purposes of key escrowing. In early 1996, the Administration expressed its intent to move forward rapidly with its proposal and to finalize export criteria and make formal conforming modifications to the export regulations "soon."

Box 5.3
Administration's Draft Software Key Escrow Export Criteria
November 1995

Key Escrow Feature

1. The key(s) required to decrypt the product's key escrow cryptographic functions' ciphertext shall be accessible through a key escrow feature.
2. The product's key escrow cryptographic functions shall be inoperable until the key(s) is escrowed in accordance with #3.
3. The product's key escrow cryptographic functions' key(s) shall be escrowed with escrow agent(s) certified by the U.S. Government, or certified by foreign governments with which the U.S. Government has formal agreements consistent with U.S. law enforcement and national security requirements.
4. The product's key escrow cryptographic functions' ciphertext shall contain, in an accessible format and with a reasonable frequency, the identity of the key escrow agent(s) and information sufficient for the escrow agent(s) to identify the key(s) required to decrypt the ciphertext.
5. The product's key escrow feature shall allow access to the key(s) needed to decrypt the product's ciphertext regardless of whether the product generated or received the ciphertext.
6. The product's key escrow feature shall allow for the recovery of multiple decryption keys during the period of

authorized access without requiring repeated presentations of the access authorization to the key escrow agent(s).

Key Length Feature

7. The product's key escrow cryptographic functions shall use an unclassified encryption algorithm with a key length not to exceed sixty-four (64) bits.
8. The product's key escrow cryptographic functions shall not provide the feature of multiple encryption (e.g., triple-DES).

Interoperability Feature

9. The product's key escrow cryptographic functions shall interoperate only with key escrow cryptographic functions in products that meet these criteria, and shall not interoperate with the cryptographic functions of a product whose key escrow encryption function has been altered, bypassed, disabled, or otherwise rendered inoperative.
Design, Implementation, and Operational Assurance
10. The product shall be resistant to anything that could disable or circumvent the attributes described in #1 through #9.

SOURCE: National Institute of Standards and Technology, Draft Software Key Escrow Encryption Export Criteria, November 6, 1995. Reprinted from text available on-line at http://csrc.ncsl.nist.gov/keyescrow/criteria.txt (November 1995 version; NIST Web page).

5.2.4 Other Federal Initiatives in Escrowed Encryption

In addition to the initiatives described above, the Administration has announced plans for new Federal Information Processing Standards in two other areas:

- FIPS-185 will be modified to include escrowed encryption for data in both communicated and stored forms. The modified FIPS is expected in late 1996; how this modification will relate to Capstone/Fortezza is as yet uncertain.
- A FIPS for key escrow will be developed that will, among other things, specify performance requirements for escrow agents and for escrowed encryption products. How this relates to the existing or modified FIPS-185 is also uncertain at this time.

Note: As this report goes to press from the prepublication version, the Administration has released a draft working paper entitled "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure"20 that appears to call for one infrastructure for cryptography that would support both public-key authentication and key-escrowing functions.

5.3 OTHER APPROACHES TO ESCROWED ENCRYPTION

A general concept akin to escrowed encryption has long been familiar to some institutions, notably banks, that have for years purchased information systems allowing them to retrieve the plaintext of encrypted files or other stored information long after the immediate need for such information has passed.21 However, only since the initial announcement of the Clipper initiative in April 1993 has escrowed encryption gained prominence in the public debate.

Denning and Branstad describe a number of different approaches to implementing an escrowed encryption scheme, all of which have been discussed publicly since 1993.22 Those and other different approaches vary along the dimensions discussed below:

- Number of escrow agents required to provide exceptional access. For example, one proposal called for separation of Clipper unit keys into more than two components.23 A second proposal called for the k-of-n arrangement described in Section 5.9.1.

- Affiliation of escrow agents. Among the possibilities are government in the executive branch, government in the judicial branch, commercial institutions, product manufacturers, and customers.
- Ability of parties to obtain exceptional access. Under the Clipper initiative, the key-escrowing feature of the EES is available only to law enforcement authorities acting under court order; users never have access to the keys.
- Authorities vested in escrow agents. In the usual discussion, escrow agents hold keys or components of keys. But in one proposal, escrow agents known as Data Recovery Centers (DRCs) do not hold user keys or user key components at all. Products escrowed with a DRC would include in the ciphertext of a transmission or a file the relevant session key encrypted with the public key of that DRC and the identity of the DRC in plaintext. Upon presentation of an

appropriate request (e.g., valid court order for law enforcement authorities, a valid request by the user of the DRC-escrowed product), the DRC would retrieve the encrypted session key, decrypt it, and give the original session key to the authorized third party, who could then recover the data encrypted with that key.24

- Hardware vs. software implementation of products.
- Partial key escrow.25 Under a partial key escrow, a product with encryption capabilities could use keys of any length, except that all but a certain number of bits would be escrowed. For example, a key might be 256 bits long, and 216 bits (256 - 40) of the key would be escrowed; 40 bits would remain private. Thus, decrypting ciphertext produced by this product would require a 256-bit work factor for those without the escrowed bits and a 40-bit work factor for those individuals in possession of the escrowed bits. Depending on the number of private bits used, this approach would protect users against disclosure of keys to those without access to the specialized decryption facilities required to conduct an exhaustive search against the private key (in this case, 40 bits).

Box 5.4 describes a number of other conceptual approaches to escrowed encryption.

Box 5.4
Non-Clipper Proposals for Escrowed Encryption

AT&T CryptoBackup. CryptoBackup is an AT&T proprietary design for a commercial or private key-escrow encryption system. The data encryption key for a document is recovered through a backup recovery vector (BRV), which is stored in the document header. The BRV contains the document key encrypted under a master public key of the escrowed agent(s). (David P. Maher, "Crypto Backup and Key Escrow," Communications of the ACM, March 1996.)

Bankers Trust Secure Key Escrow Encryption System (SecureKEES). Employees of a corporation register their encryption devices (e.g., smart card) and private encryption keys with one or more commercial escrow agents selected by the corporation. (SecureKEES product literature, CertCo, Bankers Trust Company.)

Bell Atlantic Yaksha System. An on-line key security server generates and distributes session keys and file keys using a variant of the RSA algorithm. The server transmits the keys

to authorized parties for data recovery purposes. (Ravi Ganesan, "The Yaksha Security System," Communications of the ACM, March 1996.)

Royal Holloway Trusted Third Party Services. This proposed architecture for a public key infrastructure requires that the trusted third parties associated with pairs of communicating users share parameters and a secret key. (Nigel Jefferies, Chris Mitchell, and Michael Walker, A Proposed Architecture for Trusted Third Party Services," Royal Holloway, University of London, 1995.)

RSA SecureTM. This file encryption product provides data recovery through an escrowed master public key, which can be split among up to 255 trustees using a threshold scheme. (RSA SecureTM, product literature from RSA Data Security Inc.)

Nortel Entrust. This commercial product archives users' private encryption keys as part of the certificate authority function and public-key infrastructure support. (Warwick Ford, "Entrust Technical Overview," White Paper, Nortel Secure Networks, October 1994.)

National Semiconductor CAKE. This proposal combines a TIS Commercial Key Escrow (CKE) with National Semiconductor's PersonaCardTM. (W.B. Sweet, "Commercial Automated Key Escrow (CAKE): An Exportable Strong Encryption Proposal," National Semiconductor, iPower Business Unit, June 4, 1995.)

TIS Commercial Key Escrow (CKE). This is a commercial key escrow system for stored data and file transfers. Data recovery is enabled through master keys held by a Data Recovery Center. (Stephen T. Walker, Stephen B. Lipner, Carl M. Ellison, and David M. Balenson, "Commercial Key Recovery," Communications of the ACM, March 1996.)

TECSEC VEILTM. This commercial product provides file (and object) encryption. Private key escrow is built into the key management infrastructure. (Edward M. Scheidt and Jon L. Roberts, "Private Escrow Key Management," TECSEC Inc., Vienna, Va. See also TECSEC VEILTM, product literature.)

Viacrypt PGP/BE (Business Edition). Viacrypt is a commercialized version of PGP, the free Internet-downloadable software package for encrypted communications. The Business Edition of Viacrypt optionally enables an employer to decrypt all encrypted files or messages sent or

received by an employee by carrying the session key encrypted under a "Corporate Access Key" in the header for the file or message. (See http://www.viacrypt.com.)

SOURCE: Most of these examples are taken from Dorothy Denning and Miles Smid, "Key Escrowing Today," IEEE Communications, Volume 32(9), 1994, pp. 58-68. Available on-line at http://www.cosc.georgetown.edu/~denning/crypto/Key-Escrowing-Today.txt.

5.4 THE IMPACT OF ESCROWED ENCRYPTION ON INFORMATION SECURITY

In the debate over escrowed encryption, the dimension of information security that has received the largest amount of public attention has been confidentiality. Judgments about the impact of escrowed encryption on confidentiality depend on the point of comparison. If the point of comparison is taken to be the confidentiality of data available today, then the wide use of escrowed encryption does improve confidentiality. The reason is that most information today is entirely unprotected.

Consider first information in transit (communications). Most communications today are unencrypted. For example, telephonic communications can be tapped in many different ways, including through alligator clips at a junction box in the basement of an apartment house or on top of a telephone pole, off the air when some part of a telephonic link is wireless (e.g., in a cellular call), and from the central switching office that is carrying the call. Calls made using EES-compliant telephones would be protected against such surveillance, except when surveillance parties (presumably law enforcement authorities) had obtained the necessary keys from escrow agents. As for information in storage, most files on most computers are unencrypted. Escrowed encryption applied to these files would protect them against threats such as casual snoops, although individuals with knowledge of the vulnerabilities of the system on which those files reside might still be able to access them.

On the other hand, if the point of comparison is taken to be the level of confidentiality that could be possible using unescrowed encryption, then escrowed encryption offers a lower degree of confidentiality. Escrowed encryption by

design introduces a system weakness (i.e., it is deliberately designed to allow exceptional access), and so if the procedures that protect against improper use of that access somehow fail, information is left unprotected.26 For example, EES-compliant telephones would offer less confidentiality for telephonic communications than would telephones that could be available with the same encryption algorithm and implementation but without the escrow feature, since such telephones could be designed to provide communications confidentiality against all eavesdroppers, including rogue police, private investigators, or (and this is the important point) legally authorized law enforcement officials.

More generally, escrowed encryption weakens the confidentiality provided by an encryption system by providing an access path that can be compromised.27 Yet escrowed encryption also provides a hedge against the loss of access to encrypted data by those authorized for access; for example, a user may lose or forget a decryption key. Assurances that encrypted data will be available when needed are clearly greater when a mechanism has been installed to facilitate such access. Reasonable people may disagree about how to make that trade-off in any particular case, thus underscoring the need for end users themselves to make their own risk-benefit assessments regarding the loss of authorized access (against which escrowed encryption can protect by guaranteeing key recovery) vs. the loss of confidentiality to unauthorized parties (whose likelihood is increased by the use of escrowed encryption).

A point more specifically related to EES is that escrowed encryption can also be used to enhance certain dimensions of Title III protection. For example, the final procedures for managing law enforcement access to EES-protected voice conversations call for the hardware providing exceptional access to be designed in such a way that law enforcement officials would decrypt communications only if the communications were occurring during the time window specified in the initial court authorization. The fact that law enforcement officials will have to approach escrow agents to obtain the relevant key means that there will be an audit trail for wiretaps requiring decryption, thus deterring officials who might be tempted or able to act on their own in obtaining a wiretap without legal authorization.

5.5 THE IMPACT OF ESCROWED ENCRYPTION ON

LAW ENFORCEMENT

Box 5.5 describes the requirements for escrowed encryption that law enforcement authorities (principally the FBI) would like product vendors to accommodate. But two additional high-level questions must be addressed before escrowed encryption is accepted as an appropriate solution to the stated law enforcement problem.

5.5.1 Balance of Crime Enabled vs. Crime Prosecuted

One question is the following: Does the benefit to law enforcement from access to encrypted information through an escrow mechanism outweigh the damage that might occur due to the failure of procedures intended to prevent unauthorized access to the escrow mechanism? Since government authorities believe that the implementation of these procedures can be made robust (and thus the anticipated expectation of failure is slight), they answer the question in the affirmative. Critics of government initiatives promoting escrowed encryption raise the concern that the risk of failure may be quite large, and thus their answer to the question ranges from "maybe" to "strongly negative." These parties generally prefer to rely on technologies and procedures that they fully understand and control to maintain the security of their information, and at best, they believe that any escrow procedures create a potentially serious risk of misuse that must be stringently counteracted, diligently monitored, and legally constrained. Moreover, they believe that reliance on government-established procedures to maintain proper access controls on escrowed keys invites unauthorized third parties to target those responsible for upholding the integrity of the escrow system.

History suggests that procedural risks materialize as real problems over the long run,28 but in practice, a base of operational experience is necessary to determine if these risks are significant.

Box 5.5
Law Enforcement Requirements for Escrowed Encryption Products

Information Identification

- The product is unable to encrypt/decrypt data unless the

necessary information to allow law enforcement to decrypt communications and stored information is available for release to law enforcement.
• A field is provided that readily identifies the information needed to decrypt each message, session, or file generated or received by the user of the product.
• Repeated involvement by key escrow agents (KEAs) is not required to obtain the information needed to decrypt multiple conversations and data messages (refer to expeditious information release by KEAs) during a period of authorized communications interception.

Provision of Subject's Information Only

• Only information pertaining to the communications or stored information generated by or for the subject is needed for law enforcement decryption.
Subversions of Decryption Capability
• The product is resistant against alterations that disable or bypass law enforcement decryption capabilities.
• Any alteration to the product to disable or bypass law enforcement's decryption capability requires a significant level of effort regardless of whether similar alterations have been made to any other identical version of that product.

Transparency

• The decryption of an intercepted communication is transparent to the intercept subject and all other parties to the communication except the investigative agency and the key escrow agent.
Access to Technical Details to Develop Decrypt Capability
• Law enforcement may need access to a product's technical details to develop a key escrow decrypt capability for that product.

SOURCE: Federal Bureau of Investigation, viewgraphs of presentation to International Cryptography Institute 1995 conference, September 22, 1995.

5.5.2 Impact on Law Enforcement Access to Information

Even if escrowed encryption were to achieve significant market penetration and were widely deployed, the question would still remain regarding the likely effectiveness of a law enforcement strategy to preserve wiretapping and data

recovery capabilities through deployments of escrowed encryption built around voluntary use.29 This question has surfaced most strongly in the debate over EES, but as with other aspects of the cryptography debate, the answer depends on the scenario in question:

• Many criminals will reach first for devices and tools that are readily at hand because they are so much more convenient to use than those that require special efforts to obtain. Criminals who have relatively simple and straightforward needs for secure communications may well use EES-compliant devices if they are widely available. In such cases, they will simply have forgotten (or not taken sufficient conscious account of) the fact that these "secure" devices have features that provide law enforcement access,30 and law enforcement officials will obtain the same level and quality of information they currently obtain from legal wiretaps. Indeed, the level and quality of information might be even greater than what is available today because criminals speaking on EES-compliant devices might well have a false sense of security that they could not be wiretapped.
• Criminals whose judgment suggests the need for extra and nonroutine security are likely to use secure communications devices without features for exceptional access. In these cases, law enforcement officials may be denied important information. However, the use of these communications devices is likely to be an ad hoc arrangement among participants in a criminal activity. Since many criminal activities often require participants to communicate with people outside the immediate circle of participants, "secondary" wiretap information might be available if nonsecure devices were used to communicate with others not directly associated with the activity.

Senior Administration officials have recognized that the latter scenario is inevitable--it is impossible to prevent all uses of strong unescrowed encryption by criminals and terrorists. However, the widespread deployment of strong encryption without features for exceptional access would mean that even the careless criminal would easily obtain unbreakable encryption, and thus the Administration's initiatives are directed primarily at the first scenario.

Similar considerations would apply to escrowed encryption products used to store data--many criminals will use products with encryption capabilities that are easily available to store files and send e-mail. If these products

are escrowed, law enforcement officials have a higher likelihood of having access to those criminal data files and e-mail. On the other hand, some criminals will hide or conceal their stored data through the use of unescrowed products or by storing them on remote computers whose location is known only to them, with the result that the efforts of law enforcement authorities to obtain information will be frustrated.

5.6 MANDATORY VS. VOLUNTARY USE OF ESCROWED ENCRYPTION

As noted above, the federal government cannot compel the private sector to use escrowed encryption in the absence of legislation, whether for voice communications or any other application. However, EES raised the very important public concern that the use of encryption without features for exceptional access might be banned by statute. The Administration has stated that it has no intention of outlawing the use of such cryptography or of regulating in any other way the domestic use of cryptography. Nevertheless, no administration can bind future administrations, and Congress can change a law at any time. More importantly, widespread acceptance of escrowed encryption, even if voluntary, would put into place an infrastructure that would support such a policy change. Thus, the possibility that a future administration and/or Congress might support prohibitions on unescrowed encryption cannot be dismissed. This topic is discussed in depth in Chapter 7.

With respect to the federal government's assertion of authority in the use of the EES by private parties, there are a number of gray areas. For example, a federal agency that has adopted the EES for secure telephonic communications clearly has the right to require all contractors that interact with it to use EES-compliant devices as a condition of doing business with the government;31,32 this point is explored further in Chapter 6. More problematic is the question of whether an agency that interacts with the public at large without a contractual arrangement may require such use.

A second important gray area relates to the establishment of EES as a de facto standard for use in the private sector through mechanisms described in Chapter 6. In this area, Administration officials have expressed to the committee a hope that such would be the case. If EES-compliant devices

were to become very popular, they might well drive potential competitors (specifically, devices for secure telephonic communications without features for exceptional access) out of the market for reasons of cost and scarcity. Under such circumstances, it is not clear that initially voluntary use of the EES would in the end leave room for a genuine choice for consumers.

5.7 PROCESS THROUGH WHICH POLICY ON ESCROWED ENCRYPTION WAS DEVELOPED

Much criticism of the Clipper initiative has focused on the process through which the standard was established. Specifically, the Clipper initiative was developed out of the public eye, with minimal if any connection to the relevant stakeholders in industry and the academic community, and appeared to be "sprung" on them with an announcement in the New York Times. Furthermore, a coherent approach to the international dimensions of the problem was not developed, a major failing since business communications are global in nature. After the announcement of the Clipper initiative, the federal government promulgated the EES despite a near-unanimous condemnation of the proposed standard in the public comments on it.

Similar comments have been expressed with respect to the August-September 1995 Administration proposal to relax export controls on 64-bit software products if they are properly escrowed. This proposal, advertised by the Administration as the follow-up to the Gore-Cantwell letter of July 1994,33 emerged after about a year of virtual silence from the Administration during which public interactions with industry were minimal.

The result has been a tainting of escrowed encryption that inhibits unemotional discussion of its pros and cons and makes it difficult to reach a rational and well-balanced decision.

5.8 AFFILIATION AND NUMBER OF ESCROW AGENTS

Any deployment of escrowed encryption on a large scale raises the question of who the escrow agents should be. (The equally important question of their responsibilities and liabilities is the subject of Section 5.9.) The original Clipper/Capstone escrow approach called for agencies of the executive branch to be escrow agents; at this writing, the Administration's position seems to be

evolving to allow parties in the private sector to be escrow agents. Different types of escrow agents have different advantages and disadvantages.

The use of executive branch agencies as escrow agents has a number of advantages. Executive branch escrow agents can be funded directly and established quickly, rather than depending on the existence of a private sector market or business for escrow agents. Their continuing existence depends not on market forces but on the willingness of the Congress to appropriate money to support them. Executive branch escrow agents may well be more responsive than outside escrow agents to authorized requests from law enforcement for keys. Executive branch escrow agents can be enjoined more easily from divulging to the target of a surveillance the fact that they turned over a key to law enforcement officials, thereby helping to ensure that a surveillance can be performed surreptitiously. In the case of FISA intercepts, executive branch escrow agents may be more protective of associated classified information (such as the specific target of the intercept). Under sovereign immunity, executive branch escrow agents can disavow civil liability for unauthorized disclosure of keys.

Of course, from a different standpoint, most of these putative advantages can be seen as disadvantages. If direct government subsidy is required to support an escrow operation, by definition it lacks the support of the market.34 The high speed with which executive branch escrow agents were established suggested to critics that the Administration was attempting to present the market with a fait accompli with respect to escrow. A higher degree of responsiveness to requests for keys may well coincide with greater disregard for proper procedure; indeed, since one of the designated escrow agencies (the Treasury Department) also has law enforcement jurisdiction and the authority to conduct wiretaps under some circumstances, a Treasury escrow agent might well be faced with a conflict of interest in managing keys. The obligation to keep the fact of key disclosure secret might easily lead to circumvention and unauthorized disclosures. The lack of civil liability and of criminal penalties for improper disclosure might reduce the incentives for compliance with proper procedure. Most importantly, all executive branch workers are in principle responsible to a unitary source of authority (the President). Thus, concerns are raised that any corruption at the top levels of government might diffuse downward, as exemplified by past attempts by the Executive Office of the

President to use the Internal Revenue Service to harass its political enemies. One result might be that executive branch escrow agents might divulge keys improperly; a second result might be that executive branch escrow agents could be more likely to reveal the fact of key disclosure to targets in the executive branch under investigation.

Some of the concerns described above could be mitigated by placement of escrow agents in the judiciary branch of government on the theory that since judicial approval is needed to conduct wiretaps, giving the judiciary control of escrowed keys would in fact give it a way of enforcing the Title III requirements for legal authorization. On the other hand, the judiciary branch would have to rule on procedures and misuse, thereby placing it at risk of a conflict of interest should alleged misdeeds in the judiciary branch come to light. Matters related to separation of powers between the executive and judicial branches of government are also relevant.

The best argument for government escrow agents is that government can be held politically accountable. When a government does bad things, the government can be replaced. Escrow agents must be trustworthy, and the question at root is whether it is more appropriate to trust government or a private party; the views on this point are diverse and often vigorously defended.

The committee believes that government-based escrow agents present few problems when used to hold keys associated with government work. Nonetheless, mistrust of government-based escrow agents has been one of the primary criticisms of the EES. If escrowed encryption is to serve broad social purposes across government and the private sector, it makes sense to consider other possible escrow agents in addition to government escrow agents:

- Private organizations established to provide key registration services (on a fee-for-service basis). Given that some business organizations have certain needs for data retrieval and monitoring of communications as described in Chapter 3, such needs might create a market for private escrow agents. Some organizations might charge more and provide users with bonding against failure or improper revelations of keys; other organizations might charge less and not provide such bonding.
- Vendors of products with encryption capabilities and features for exceptional access. Vendors acting as escrow

agents would face a considerable burden in having to comply with registration requirements and might be exposed to liability.35 At the same time, vendors could register keys at the time of manufacture or by default at some additional expense.36

• Customers themselves. In the case of a corporate customer, a specially trusted department within the corporation that purchases escrowed encryption products could act as an escrow agent for the corporation. Such "customer escrow" of a corporation's own keys may be sufficient for its needs; customer escrow would also enable the organization to know when its keys have been revealed. Since legal entities such as corporations will continue to be subject to extant procedures of the law enforcement court order or subpoena, law enforcement access to keys under authorized circumstances could be assured. In the case of individual customers who are also the end users of the products they purchase, the individual could simply store a second copy of the relevant keys as a form of customer escrow.

Note especially that site licenses37 to corporations account for the largest portion of vendor sales in software.38 In a domestic context, corporations are entities that are subject to legal processes in the United States that permit law enforcement authorities to obtain information in the course of a criminal investigation. In a foreign context, exports to certain foreign corporations can be conditioned on a requirement that the foreign corporation be willing to escrow its key in such a manner that U.S. law enforcement authorities would be able to have access to that information under specified circumstances and in a manner to be determined by a contract binding on the corporation. (The use of contract law in this manner is discussed further in Chapter 7.) In short, sales of escrowed encryption to foreign and domestic corporate users could be undertaken in such a way that a very large fraction of the installed user base would in fact be subject to legal processes for obtaining information on keys.

Nongovernment escrow agents are subject to the laws of the government under whose jurisdiction they operate. In addition, they raise other separate questions. For example, a criminal investigation may target the senior officials of a corporation, who may themselves be the ones authorized for access to customer-escrowed keys; they might then be notified of the fact of being wiretapped. The same would be true of end users controlling their own copies of keys.

Private organizations providing key-holding services might be infiltrated or even set up by criminal elements that would frustrate lawful attempts to obtain keys or would even use the keys in their possession improperly. Private organizations may be less responsive to government requests than government escrow agents. Finally, private organizations motivated by profit and tempted to cut corners might be less responsible in their conduct.

A second important issue regarding escrow agents deals with their number. Concentrating escrow arrangements in a few escrow agents may make law enforcement access to keys more convenient, but it also focuses the attention of those who may attempt to compromise those facilities--the "big, fat target" phenomenon--because the aggregate value of the keys controlled by these few agents is, by assumption, large.39 On the other hand, given a fixed budget, concentrating resources on a few escrow agents may enable them to increase the security against compromise, whereas spreading resources among many escrow agents may leave each one much more open to compromise. Indeed, the security of a well-funded and well-supported escrow agent may be greater than that of the party that owns the encryption keys; in this case, the incremental risk that a key would be improperly compromised by the escrow agent would be negligible. Increasing the number of escrow agents so that each would be responsible for a relatively small number of keys reduces the value of compromising any particular escrow agent but increases the logistical burdens, overhead, and expense for the nation. The net impact on security against compromise of keys is very scenario-dependent.40

5.9 RESPONSIBILITIES AND OBLIGATIONS OF ESCROW AGENTS AND USERS OF ESCROWED ENCRYPTION

Regardless of who the escrow agents are, they will hold certain information and have certain responsibilities and obligations.41 Users of escrowed encryption also face potential liabilities.

5.9.1 Partitioning Escrowed Information

Consider what precisely an escrow agent would hold. In the simplest case, a single escrow agent would hold all of the information needed to provide exceptional access to encrypted information. (In the Clipper case, two escrow agents would be used to hold the unit keys to all EES-compliant telephones.)

A single escrow agent for a given key poses a significant risk of single-point failure--that is, the compromise of only one party (the single escrow agent) places at risk all information associated with that key. The Clipper/Capstone approach addresses this point by designating two executive branch agencies (Commerce and Treasury), each holding one component (of two) of the unit key of a given Clipper/Capstone-compliant device. Reconstruction of a unit key requires the cooperation of both agencies. This approach was intended to give the public confidence that their keys were secure in the hands of the government.

In the most general case, an escrow system can be designed to separate keys into n components but with the mathematics of the separation process arranged so that exceptional access would be possible if the third party were able to acquire any k (for k less than or equal to n) of these components.42 This approach is known as the "k-of-n" approach. For the single escrow agent, k = 1 and n = 1; for the Clipper/Capstone system, k = 2 and n = 2. But it is possible to design systems where k is any number less than n; for example, the consent of any three (k) of five (n) escrow agents could be sufficient to enable exceptional access. Obviously, the greater the number of parties that are needed to consent, the more cumbersome exceptional access becomes.

It is a policy or business decision as to what the specific values of k and n should be, or if indeed the choice about specific values should be left to users. The specific values chosen for k and n reflect policy judgments about needs for recovery of encrypted data relative to user concerns about improper exceptional access. Whose needs? If a national policy decision determines k and n, it is the needs of law enforcement and national security weighed against user concerns. If the user determines k and n, it is the needs of the user weighed against law enforcement and national security concerns.

5.9.2 Operational Responsibilities of Escrow Agents

For escrowed encryption to play a major role in protecting the information infrastructure of the nation and the information of businesses and individuals, users must be assured about the operational obligations and procedures of escrow agents. Clear guidelines will be required to regulate the operational behavior of escrow agents, and

clear enforcement mechanisms must be set into place to ensure that the escrow agents comply with those guidelines. While these guidelines and mechanisms might come into existence through normal market forces or cooperative agreements within industries, they are more likely to require a legal setting that would also include criminal penalties for malfeasance.

Guidelines are needed to assure the public and law enforcement agencies of two points:

- That information relevant to exceptional access (the full key or a key fragment) will be divulged upon proper legal request and that an escrow agent will not notify the key owner of disclosure until it is legally permissible to do so, and
- That information relevant to exceptional access will be divulged only upon proper legal request.

Note that the fulfillment of the second requirement has both an "abuse of authority" component and a technical and procedural component. The first relates to an individual (an "insider") who is in a position to give out relevant information but also to abuse his position by giving out that information without proper authorization. The second relates to the fact that even if no person in the employ of an escrow agent improperly gives out relevant information, an "outsider" may be able to penetrate the security of the escrow agent and obtain the relevant information without compromising any particular individual. Such concerns are particularly relevant to the extent that escrow agents are connected electronically, since they would then be vulnerable in much the same ways that all other parties connected to a network are vulnerable. The security of networked computer systems is difficult to assure with high confidence,43 and the security level required of escrow agents must be high, given the value of their holdings to unauthorized third parties.

Thus, those concerned about breaches of confidentiality must be concerned about technical and procedural weaknesses of the escrow agent infrastructure that would enable outsiders to connect remotely to these sites and obtain keys, as well as about insiders abusing their positions of trust. Either possibility could lead not just to individual keys being compromised, but also to wholesale compromise of all of the keys entrusted to escrow agents within that infrastructure. From a policy standpoint, it is necessary to have a

contingency plan that would facilitate recovery from wholesale compromise.

Box 5.6 describes law enforcement views on the responsibilities of escrow agents. Box 5.7 describes draft Administration views on requirements for maintaining the integrity and security of escrow agents; Box 5.8 describes draft Administration views on requirements for assuring access to escrowed keys.

Box 5.6
Law Enforcement Requirements for Escrow Agents
Information Availability

• The information necessary to allow law enforcement the ability to decrypt communications and stored information is available. KEAs [key escrow agents] should maintain or be capable of generating all the necessary decrypt (key) information.
• Key and/or related information needed to decrypt communications and stored information is retained for extended time periods. KEAs should be able to decrypt information encrypted with a device or product's current and/or former key(s) for a time period that may vary depending on the application (e.g., voice vs. stored files).
• A backup capability exists for key and other information needed to decrypt communications and stored information. Thus, a physically separate backup capability should be available to provide redundancy of resources should the primary capability fail.

Key Escrow Agent (KEA) Accessibility

• KEAs should be readily accessible. For domestic products, they should reside and operate in the United States. They should be able to process proper requests at any time; most requests will be submitted during normal business hours, but exigent circumstances (e.g., kidnappings, terrorist threats) may require submission of requests during nonbusiness hours.

Information Release by KEAs

• The information needed for decryption is expeditiously released upon receipt of a proper request. Since communications intercepts require the ability to decrypt multiple conversations and data messages sent to or from the

subject (i.e., access to each session or message key) during the entire intercept period, only one initial affirmative action should be needed to obtain the relevant information. Exigent circumstances (e.g., kidnappings, terrorist threats) will require the release of decrypt information within a matter of hours.

Confidentiality and Safeguarding of Information

• KEAs should safeguard and maintain the confidentiality of information pertaining to the request for and the release of decrypt information. KEAs should protect the confidentiality of the person or persons for whom a key escrow agent holds keys or components thereof, and protect the confidentiality of the identity of the agency requesting decrypt information or components thereof and all information concerning such agency's access to and use of encryption keys or components thereof.

For law enforcement requests, KEA personnel knowledgeable of an interception or decryption should be of good character and have not been convicted of crimes of moral turpitude or otherwise bearing on their trustworthiness. For national security requests, KEA personnel viewing and/or storing classified requests must meet the applicable U.S. government requirements for accessing and/or storing classified information. Efforts are ongoing to examine unclassified alternatives.

• KEAs should be legitimate organizations without ties to criminal enterprises, and licensed to conduct business in the United States. KEAs for domestic products should not be a foreign corporation, a foreign country, or an entity thereof.

SOURCE: Federal Bureau of Investigation, viewgraphs of presentation to International Cryptography Institute 1995 conference, September 22, 1995.

Box 5.7
Proposed U.S. Government Requirements for Ensuring Escrow Agent Integrity and Security

1. Escrow agent entities shall devise and institutionalize policies, procedures, and mechanisms to ensure the confidentiality, integrity, and availability of key escrow related information.

a. Escrow agent entities shall be designed and operated so that a failure by a single person, procedure, or mechanism does not compromise the confidentiality, integrity or availability of the key and/or key components (e.g., two person control of keys, split keys, etc.)
b. Unencrypted escrowed key and/or key components that are stored and/or transmitted electronically shall be protected (e.g., via encryption) using approved means.
c. Unencrypted escrowed key and/or key components stored and/or transferred via other media/methods shall be protected using approved means (e.g., safes).
2. Escrow agent entities shall ensure due form of escrowed key access requests and authenticate the requests for escrowed key and/or key components.
3. Escrow agent entities shall protect against disclosure of information regarding the identity of the person/organization whose key and/or key components is requested, and the fact that a key and/or key component was requested or provided.
4. Escrow agent entities shall enter keys/key components into the escrowed key database immediately upon receipt.
5. Escrow agent entities shall ensure at least two copies of any key and/or key component in independent locations to help ensure the availability of such key and/or key components due to unforeseen circumstances.
6. Escrow agent entities that are certified by the U.S. government shall work with developers of key escrow encryption products and support a feature that allows products to verify to one another that the products' keys have been escrowed with a U.S.-certified agent.

SOURCE: National Institute of Standards and Technology, Draft Key Escrow Agent Criteria, December 1, 1995. Reprinted from text available on-line at http://csrc.ncsl.nist.gov/keyescrow/criteria.txt.

5.9.3 Liabilities of Escrow Agents

In order to assure users that key information entrusted to escrow agents remains secure and authorized third parties that they will be able to obtain exceptional access to encrypted data when necessary, escrow agents and their employees must be held accountable for improper behavior and for the use of security procedures and practices that are appropriate to the task of protection.

Box 5.8
Proposed Requirements for Ensuring Key Access

7. An escrow agent entity shall employ one or more persons who possess a SECRET clearance for purposes of processing classified (e.g., FISA) requests to obtain keys and/or key components.
8. Escrow agent entities shall protect against unauthorized disclosure of information regarding the identity of the organization requesting the key or key components.
9. Escrow agent entities shall maintain data regarding all key escrow requests received, key escrow components released, database changes, system administration accesses, and dates of such events, for purposes of audit by appropriate government officials or others.
10. Escrow agent entities shall maintain escrowed keys and/or key components for as long as such keys may be required to decrypt information relevant to a law enforcement investigation.
11. Escrow agent entities shall provide key/key components to authenticated requests in a timely fashion and shall maintain a capability to respond more rapidly to emergency requirements for access.
12. Escrow agent entities shall possess and maintain a Certificate of Good Standing from the State of incorporation (or similar local/national authority).
13. Escrow agent entities shall provide to the U.S. government a Dun & Bradstreet/TRW number or similar credit report pointer and authorization.
14. Escrow agent entities shall possess and maintain an Errors & Omissions insurance policy.
15. Escrow agent entities shall provide to the U.S. government a written copy of, or a certification of the existence of a corporate security policy governing the key escrow agent entity's operation.
16. Escrow agent entities shall provide to the U.S. government a certification that the escrow agent will comply with all applicable federal, state, and local laws concerning the provisions of escrow agent entity services.
17. Escrow agent entities shall provide to the U.S. government a certification that the escrow agent entity will transfer to another approved escrow agent the escrow agent entity's equipment and data in the event of any dissolution or other cessation of escrow agent entity operations.
18. Escrow agent entities for products sold in the United States shall not be a foreign country or entity thereof, a national of a foreign country, or a corporation of which an alien is an officer or more than one-fourth of the stock

which is owned by aliens or which is directly or indirectly controlled by such a corporation. Foreign escrow agent entities for products exported from the United States will be approved on a case by case basis as law enforcement and national security agreements can be negotiated.
19. Escrow agent entities shall provide to the U.S. government a certification that the escrow agent entity will notify the U.S. government in writing of any changes in the forgoing information.
20. Fulfillment of these and the other criteria are subject to periodic recertification.

NOTE: The material reprinted in this box is a continuation of the requirements listed in Box 5.7 and is extracted from the same source.

Liabilities can be criminal or civil (or both). For example, criminal penalties could be established for the disclosure of keys or key components to unauthorized parties or for the refusal to disclose such information to appropriately authorized parties. It is worth noting that the implementing regulations accompanying the EES proposal run counter to this position in the sense that they do not provide specific penalties for failure to adhere to the procedures for obtaining keys (which only legislation could do). The implementing regulations specifically state that "these procedures do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance, and noncompliance with these procedures shall not provide the basis for any motion to suppress or other objection to the introduction of electronic surveillance evidence lawfully acquired."44

Questions of civil liability are more complex. Ideally, levels of civil liability for improper disclosure of keys would be commensurate with the loss that would be incurred by the damaged party. For unauthorized disclosure of keys that encrypt large financial transactions, this level is potentially very large.45 On the other hand, as a matter of public policy, it is probably inappropriate to allow such levels of damages. More plausible may be a construct that provides what society, as expressed through Congress, thinks is reasonable (Box 5.9). Users of escrow agents might also be able to buy their own insurance against unauthorized disclosure. Note that holding government agencies liable for civil damages might require an explicit change in the Federal Tort Claims Act that waives sovereign immunity in

certain specified instances, or other legislative changes.

On the other hand, the amount of liability associated with compromising information related to data communications is likely to dwarf the analogous volume for voice communications. If escrowed encryption is adopted widely in data communications, compromise of escrow agents holding keys relevant to network encryption may be catastrophic, and may become easier as the number of access points that can be penetrated becomes larger.

Box 5.9
Statutory Limitations on Liability

Government can promote the use of specific services and products by assuming some of the civil liability risks associated with them. Three examples follow:

- The Atomic Energy Damages Act, also called the Price-Anderson Act, limits the liability of nuclear power plant operators for harm caused by a nuclear incident (such as an explosion or radioactive release). To operate a nuclear power plant, a licensee must show the U.S. Nuclear Regulatory Commission (U.S. NRC) that it maintains financial protection (such as private insurance, self-insurance, or other proof of financial responsibility) equal to the maximum amount of insurance available at reasonable cost and reasonable terms from private sources, unless the U.S. NRC sets a lower requirement on a case-specific basis. The U.S. NRC indemnifies licensees from all legal liability arising from a nuclear incident, including a precautionary evacuation, which is in excess of the required financial protection, up to a maximum combined licensee-and-government liability of $560 million. Incidents that cause more than $560 million in damage will trigger review by the Congress to determine the best means to compensate the public, including appropriating funds.
- The Commercial Space Launch Act provides similar protection to parties licensed to launch space vehicles or operate launch sites, but with a limit on the total liability the United States accepts. The licensee must obtain financial protection sufficient to compensate the maximum probable loss that third parties could claim for harm or damage, as determined by the secretary of transportation. The most that can be required is $500 million or the maximum liability insurance available from private sources, whichever is lower. The United States is

obligated to pay successful claims by third parties in excess of the required protection, up to $1.5 billion, unless the loss is related to the licensee's willful misconduct. The law also requires licensees to enter into reciprocal waivers of claims with their contractors and customers, under which each party agrees to be responsible for losses it sustains.

- The swine flu vaccination program of 1976 provides an example in which the United States accepted open-ended liability and paid much more than expected. Doctors predicted a swine flu epidemic, and Congress appropriated money for the Department of Health, Education, and Welfare (HEW) to pay four pharmaceutical manufacturers for vaccines to be distributed nationwide. The manufacturers' inability to obtain liability insurance delayed the program until Congress passed legislation (P.L. 94-380) in which the United States assumed all liability other than manufacturer negligence. The government's liability could thus include, for example, harmful side effects. Claims against the United States would be processed under the Federal Tort Claims Act (which provides for trial by judge rather than jury and no punitive damages, among other distinctions). Some of the 45 million people who were immunized developed complications, such as Guillain-Barre syndrome; consequently, the program was canceled. By September 1977, 815 claims had been filed. The United States ultimately paid more than $100 million to settle claims, and some litigation is still pending today. Manufacturers, who by law were liable only for negligence, were not sued.

Note that liability of escrow agents may be related to the voluntary use of escrow. A party concerned about large potential losses would have alternatives to escrowed encryption--namely, unescrowed encryption--that would protect the user against the consequences of improper key disclosure. Under these circumstances, a user whose key was compromised could be held responsible for his loss because he did not choose to use unescrowed encryption; an escrow agent's exposure to liability would be limited to the risks associated with parties that use its services. On the other hand, if escrowed encryption were the only cryptography permitted to be used, then by assumption the user would have no alternatives, and so in that case an escrow agent would shoulder a larger liability.

Another aspect of liability could arise if the escrow agents were also charged with the responsibilities of certificate

authorities. Under some circumstances, it might be desirable for the functions of escrow agents and certificate authorities to be carried out by the same organization. Thus, these dual-purpose organizations would have all of the liabilities carried by those who must certify the authenticity of a given party.

5.10 THE ROLE OF SECRECY IN ENSURING PRODUCT SECURITY

The fact that EES and the Fortezza card involve classified algorithms has raised the general question of the relationship between secrecy and the maintenance of a product's trustworthiness in providing security. Specifically, the Clipper/Capstone approach is based on a secret (classified) encryption algorithm known as Skipjack. In addition, the algorithm is implemented in hardware (a chip) whose design is classified. The shroud of secrecy surrounding the hardware and algorithms needed to implement EES and Fortezza makes skeptics suspect that encrypted communications could be decrypted through some secret "back door" (i.e., without having the escrowed key).46

Logically, secrecy can be applied to two aspects of an encryption system: the algorithms used and the nature of the implementation of these algorithms. Each is addressed in turn below. Box 5.10 describes a historical perspective on cryptography and secrecy that is still valid today.

Box 5.10
Perspectives on Secrecy and System Security

The distinction between the general system (i.e., a product) and the specific key (of an encrypted message) was first articulated by Auguste Kerckhoffs in his historic book La Cryptographie Militaire, published in 1883. Quoting David Kahn in The Codebreakers:

Kerckhoffs deduced [that] . . . compromise of the system should not inconvenience the correspondents. . . . Perhaps the most startling requirement, at first glance, was the second . . . . Kerckhoffs explained that by "system" he meant "the material part of the system; tableaux, code books, or whatever mechanical apparatus may be necessary," and not "the key proper." Kerckhoffs here makes for the first time the distinction, now basic to cryptology, between the general system and the specific key. Why must the

general system "not require secrecy"? . . . "Because," Kerckhoffs said, "it is not necessary to conjure up imaginary phantoms and to suspect the incorruptibility of employees or subalterns to understand that, if a system requiring secrecy were in the hands of too large a number of individuals, it could be compromised at each engagement. . . . This has proved to be true, and Kerckhoffs' second requirement has become widely accepted under a form that is sometimes called the fundamental assumption of military cryptography: that the enemy knows the general system. But he must still be unable to solve messages in it without knowing the specific key. In its modern formulation, the Kerckhoffs doctrine states that secrecy must reside solely in the keys."1

A more modern expression of this sentiment is provided by Dorothy Denning:

The security of a cryptosystem should depend only on the secrecy of the keys and not on the secrecy of the algorithms. . . . This requirement implies the algorithms must be inherently strong; that is, it should not be possible to break a cipher simply by knowing the method of encipherment. This requirement is needed because the algorithms may be in the public domain, or known to a cryptanalyst.2

1David Kahn, The Codebreakers, MacMillan, New York, 1967, p. 235.
2Dorothy Denning, Cryptography and Data Security, Addison-Wesley, Reading, Mass., 1982, p. 8.

5.10.1 Algorithm Secrecy

The use of secret algorithms for encryption has advantages and disadvantages. From an information security standpoint, a third party who knows the algorithm associated with a given piece of ciphertext has an enormous advantage over one who does not--if the algorithm is unknown, cryptanalysis is much more difficult. Thus, the use of a secret algorithm by those concerned about information security presents an additional (and substantial) barrier to those who might be eavesdropping. From a signals intelligence (SIGINT) standpoint, it is advantageous to keep knowledge of good encryption out of the hands of potential SIGINT targets. Thus, if an algorithm provides good cryptographic security, keeping the algorithm secret prevents the SIGINT target from

implementing it. In addition, if an algorithm is known to be good, studying it in detail can reveal a great deal about what makes any algorithm good or bad. Algorithm secrecy thus helps to keep such information out of the public domain.47

On the other hand, algorithm secrecy entails a number of disadvantages as well. One is that independent analysis of a secret algorithm by the larger community is not possible. Without such analysis, flaws may remain in the algorithm that compromise the security it purports to provide. If these flaws are kept secret, users of the algorithm may unknowingly compromise themselves. Even worse, sophisticated users who need high assurances of security are unable to certify for themselves the security it provides (and thus have no sense of the risks they are taking if they use it). In most cases, the real issue is whether the user chooses to rely on members of the academic cryptography communities publishing in the open literature, or on members of the classified military community or members of the commercial cryptography community who are unable to fully disclose what they know about a subject because it is classified or proprietary.

A second disadvantage of algorithm secrecy is the fact that if a cryptographic infrastructure is based on the assumption of secrecy, public discovery of those secrets can compromise the ends to be served by that infrastructure. For example, if a cryptographic infrastructure based on a secret algorithm were widely deployed, and if that algorithm contained a secret and unannounced "back door" that allowed those with knowledge of this back door easy access to encrypted data, that infrastructure would be highly vulnerable and could be rendered untrustworthy in short order by the public disclosure of the back door.

A third disadvantage is that a secret algorithm cannot be implemented in software with any degree of assurance that it will remain secret. Software, as it exists ready for actual installation on a computer (so-called object code or executable code), can usually be manipulated with special software tools to yield an alternate form (namely, source code) reflecting the way the creating programmer designed it, and therefore revealing many, even most, of its operational details, including any algorithm embedded within it. This process is known as "decompiling" or "disassembly" and is a standard technique in the repertoire of software engineers.48

All of the previous comments apply to secrecy whether it is the result of government classification decisions or vendor choices to treat an algorithm as a trade secret. In addition, vendors may well choose to treat an algorithm as a trade secret to obtain the market advantages that proprietary algorithms often bring. Indeed, many applications of cryptography for confidentiality in use today are based on trade-secret algorithms such as RC2 and RC4.

5.10.2 Product Design and Implementation Secrecy

Product design and implementation secrecy has a number of advantages. For example, by obscuring how a product has been designed, secrecy makes it more difficult for an outsider to reverse-engineer the product in such a way that he could understand it better or, even worse, modify it in some way. Since vulnerabilities sometimes arise in implementation, keeping the implementation secret makes it harder for an attacker to discover and then exploit those vulnerabilities. Design and implementation secrecy thus protects any secrets that may be embedded in the product for a longer time than if they were to be published openly.

On the other hand, it is taken as an axiom by those in the security community that it is essentially impossible to maintain design or implementation secrecy indefinitely. Thus, the question of the time scale of reverse engineering is relevant--given the necessary motivation, how long will it take and how much in resources will be needed to reverse-engineer a chip or a product?

- For software, reverse engineering is based on decompilation or disassembly (as described in Section 5.10.1). The larger the software product, the longer it takes to understand the original program; even a small one can be difficult to understand, especially if special techniques have been used to obscure its functionality. Modification of the original program can present additional technical difficulties (the product may be designed in such a way that disassembling or decompiling the entire product is necessary to isolate critical features that one might wish to modify). Certain techniques can be used to increase the difficulty of making such modifications,49 but there is virtual unanimity in the computer community that modification cannot be prevented forever. How robust must these anti-reverse-engineering features be? The answer is

that they must be robust enough that the effort needed to overcome them is greater than the effort needed to develop an encryption system from scratch.

• For hardware, reverse engineering takes the form of physical disassembly and/or probing with x-rays of the relevant integrated circuit chips. Such chips can be designed to resist reverse engineering in a way that makes it difficult to understand what various components on the chip do. For example, the coating on a die used to fabricate a chip may be designed so that removal of the coating results in removal of one or more layers of the chip, thus destroying portions of what was to be reverse-engineered. The chip may also be fabricated with decoy or superfluous elements that would distract a reverse engineer. For all of these reasons, reverse engineering for understanding a chip's functions is difficult. However, it is not impossible, and under some circumstances, it is possible to modify a chip. In general, reverse engineering of the circuits and devices inside a chip requires significant expertise and access to expensive tools.50

An important factor that works against implementation secrecy is the wide distribution of devices or products whose implementation is secret. It is difficult to protect a device against reverse engineering when millions of those devices are distributed around the world without any physical barriers (except those on the implementation itself) to control access to them. Everyone with an EES-compliant telephone or a Foretzza card, for example, will have access to the chip that provides encryption and key escrow services.

The comments above refer to the feasibility of maintaining implementation secrecy. But there are issues related to its desirability as well. For example, implementation secrecy implies that only a limited number of vendors can be trusted to produce a given implementation. Thus, foreign production of Clipper/Capstone-compliant devices under classification guidelines raises problems unless foreign producers are willing to abide by U.S. security requirements.

A more important point is that implementation secrecy also demands trust between user and supplier/vendor. Users within government agencies generally trust other parts of the government to provide adequate services as a supplier. But in the private sector, such trust is not necessarily warranted. Users that are unable to determine for themselves what algorithms are embedded in computer and

communications products used must trust the vendor to have provided algorithms that do what the user wants done, and the vast majority of users fall into this category. Such opacity functions as a de facto mechanism of secrecy that also impedes user knowledge about the inner workings and that is exploited by the distributors of computer viruses and worms. As a result, choosing between self-implemented source code and a prepackaged program for use in performing certain functions is in many ways analogous to choosing between unclassified and classified algorithms.

An information security manager with very high security needs must make trade-offs in assurance vs. cost. In general, the only way to be certain that the algorithms used are the ones claimed to be used is to implement them on one's own. Yet if a manager lacks the necessary knowledge and experience, a self-implementation may not be as secure or as capable as one developed by a trusted vendor. A self-implementer also carries the considerable burden of development costs that a commercial vendor can amortize over many sales.

As a result, security-conscious users of products whose inner workings are kept secret must (1) trust the vendor implicitly (based on factors such as reputation), or (2) face the possibility of various extreme scenarios. Here are two:

- The hardware of a secret device can be dynamically modified; for example, electrically erasable read-only memories can direct the operation of a processor. One possible scenario with secret hardware is that a chip that initially provides Clipper-chip functionality might be reprogrammed when it first contacts a Clipper/Capstone-compliant device to allow nonescrowed but unauthorized access to it; such a means of "infection" is common with computer viruses. In other words, the Skipjack algorithm may have been embedded in the chip when it was first shipped, but after the initial contact, the algorithm controlling the chip is no longer Skipjack.
- An algorithm that is not Skipjack is embedded by the manufacturer in chips purporting to be Clipper or Capstone chips. Since the utility of a vector test depends on the availability of an independent implementation of the algorithm, it is impossible for the user to perform this test independently if the user has no reference point. As a result, the user has no access to an independent test of the chip that is in the user's "Clipper/Capstone-compliant"

device, and so any algorithm might have been embedded.51

Any technically trained person can invent many other such scenarios. Thus, public trust in the technical desirability of the EES and Fortezza for exceptional access depends on a high degree of trust in the government, entirely apart from any fears about compromising escrow agents wherever they are situated.

Of course, some of the same considerations go beyond the Skipjack algorithm and the Clipper/Capstone approach. In general, users need confidence that a given product with encryption capabilities indeed implements a given algorithm. Labeling a box with the letters "DES" does not ensure that the product inside really implements DES. In this case, the fact that the DES algorithm is publicly known facilitates testing to verify that the algorithm is implemented correctly.52 If its source code is available for inspection, other security-relevant aspects of a software product can be examined to a certain extent, at least up to the limits of the expertise of the person checking the source code. But for software products without source code, and especially for hardware products that cannot easily be disassembled, and even more so for hardware products that are specifically designed to resist disassembly, confidence in the nonalgorithm security aspects of the product is more a matter of trusting the vendor than of the user making an independent technical verification of an implementation.53 In some sectors (e.g., banking, classified military applications), however, independent technical verification is regarded as essential.

Finally, a given product may properly implement an algorithm but still be vulnerable to attacks that target the part of the product surrounding the implementation of the algorithm. Such vulnerabilities are most common in the initial releases of products that have not been exposed to public test and scrutiny. For example, a security problem with the Netscape Navigator's key-generation facility could have been found had the implementation in which the key generator was embedded been available for public examination prior to its release, even though the encryption algorithm itself was properly implemented.54

5.11 THE HARDWARE-SOFTWARE CHOICE IN PRODUCT IMPLEMENTATION

After the Clipper initiative was announced, and as the

debate over escrowed encryption broadened to include the protection of data communications and stored data, the mass market software industry emphasized that a hardware solution to cryptographic security--as exemplified by the Clipper chip--would not be satisfactory. The industry argued with some force that only a software-based approach would encourage the widespread use of encryption envisioned for the world's electronic future, making several points:

- Customers have a strong preference for using integrated cryptographic products. While stand-alone products with encryption capabilities could be made to work, in general they lack operational convenience for the applications that software and systems vendors address.
- Compared to software, hardware is expensive to manufacture. In particular, the relevant cost is not simply the cost of the hardware encryption device compared to a software encryption package,55 but also the cost of any modifications to the hardware environment needed to accept the hardware encryption device.56 For example, one major company noted to the committee that adoption of the Fortezza card, a card that fits into the PC-card slots available on most laptop computers, would be very expensive in its desktop computing environment, because most of its desktop computers do not have a PC-card slot and would have to be modified to accept the Fortezza card. By contrast, a software encryption product can simply be loaded via common media (e.g., a CD-ROM or a floppy disk) or downloaded via a network.
- The fact that hardware is difficult to change means that problems found subsequent to deployment are more difficult to fix. For example, most users would prefer to install a software fix by loading a CD-ROM into their computers than to open up their machines to install a new chip with a hardware fix.
- Hardware-based security products have a history of being market-unfriendly. Hardware will, in general, be used only to the extent that the required hardware (and its specific configuration) is found in user installations. Moreover, hardware requirements can be specified for software only when that hardware is widely deployed. For example, a technical approach to the software piracy problem has been known for many years; the approach requires the installation of special-purpose hardware that is available only to those who obtain the software legitimately. This "solution" has failed utterly in the marketplace, and software piracy remains a multibillion-dollar-per-year problem.
- Hardware for security consumes physical space and power

in products. For example, a hardware-based encryption card that fits into an expansion slot on a computer takes up a slot permanently, unless the user is willing to install and deinstall the card for every use. It also creates an additional power demand on electronic devices where power and battery life are limited.

In general, products with encryption capabilities today use software or hardware or both to help ensure security.57 The crux of the hardware-software debate is what is good enough to ensure security. The security needed to manage electronic cash in the international banking system needs to be much stronger than the security to protect word processing files created by private individuals. Thus, software-based cryptography might work for the latter, while hardware-based cryptography might be essential for the former.

Products with encryption capabilities must be capable of resisting attack. But since such products are often embedded in operating environments that are themselves insecure, an attacker may well choose to attack the environment rather than the product itself. For example, a product with encryption capabilities may be hardware-based, but the operating environment may leave the encryption keys or the unencrypted text exposed.58 More generally, in an insecure environment, system security may well not depend very much on whether the cryptography per se is implemented in hardware or software or whether it is weak or strong.

In the context of escrowed encryption, a second security concern arises--a user of an escrowed encryption product may wish to defeat the escrow mechanism built into the product. Thus, the escrow features of the product must be bound to the product in a way that cannot be bypassed by some reverse-engineered modification to the product. This particular problem is known as binding or, more explicitly, escrow binding; escrow binding is an essential element of any escrow scheme that is intended to provide exceptional access.

Concern over how to solve the escrow binding problem was the primary motivation for the choice of a hardware approach to the Clipper initiative. As suggested in Section 5.10, the functionality of a hardware system designed to resist change is indeed difficult to change, and so hardware implementations have undeniable advantages for solving the escrow binding problem.59 An EES-compliant device would be

a telephone without software accessible to the user, and would provide high assurance that the features for exceptional access would not be bypassed.

As the debate has progressed, ideas for software-based escrow processes have been proposed. The primary concern of the U.S. government about software implementations is that once a change has been designed and developed that can bypass the escrow features ("break the escrow binding"), such a change can be easily propagated through many different channels and installed with relatively little difficulty. In the committee's view, the important question is whether software solutions to the escrow binding problem can provide an acceptable level of protection against reverse engineering. Whether an escrowed encryption product is implemented in software (or hardware for that matter), the critical threshold is the difficulty of breaking the escrow binding (i.e., bypassing the escrowing features) compared to the effort necessary to set up an independent unescrowed encryption system (perhaps as part of an integrated product). If it is more difficult to bypass the escrow features than to build an unescrowed system, then "rogues" who want to defeat exceptional access will simply build an unescrowed system. The bottom line is that an escrowed encryption product does not have to be perfectly resistant to breaking the escrow binding.

A possible mitigating factor is that even if a software "patch" is developed that would break the escrow binding of an escrowed encryption software product, it may not achieve wide distribution even among the criminals who would have the most to gain from such a change. Experience with widely deployed software products (e.g., operating systems) indicates that even when a software fix is made available for a problem in a product, it may not be implemented unless the anomalous or incorrect software behavior is particularly significant to an end user. If this is the case for products that are as critical as operating systems, it may well be true for products with more specialized applications. On the other side of the coin, many parties (e.g., criminals) may care a great deal about the presence of escrowing and thus be highly motivated to find "fixes" that eliminate escrowing.

5.12 RESPONSIBILITY FOR GENERATION OF UNIT KEYS

Key generation is the process by which cryptographic keys are generated. Two types of keys are relevant:

• A session key is required for each encryption of plaintext into ciphertext; this is true whether the information is to be stored or communicated. Ultimately, the intended recipients of this information (those who retrieve it from storage or those who receive it at the other end of a communications channel) must have the same session key. For maximum information security, a new session key is used with every encryption. (See footnote 7 of this chapter for more discussion.)
• A unit key is a cryptographic key associated with a particular product or device owned or controlled by a specific individual. Unit keys are often used to protect session keys from casual observation in escrowed encryption products, but precisely how they are used depends on the specifics of a given product.

In the most general case, the session key is a random number, and a different one is generated anew for each encryption. But the unit key is a cryptographic variable that typically changes on a much longer time scale than does the session key. In many escrowed encryption schemes, knowledge of the unit key enables a third party to obtain the session key associated with any given encryption.

The Clipper/Capstone approach requires that the unit key be generated by the manufacturer at the time of manufacture ("at birth") and then registered prior to sale with escrow agents in accordance with established procedures. Such an approach has one major advantage from the standpoint of those who may require exceptional access in the future--it guarantees registration of keys, because users need not take any action to ensure registration.

At the same time, since the Clipper/Capstone approach is based on a hardware-based implementation that is not user-modifiable, a given device has only one unit key for its entire lifetime, although, at some cost, the user may change the Clipper chip embedded in the device.60 If the unit key is compromised, the user's only recourse is to change the chip. A user who does not do so violates one basic principle of information security--frequent changing of keys (or passwords).61 In addition, the fact that all unit keys are known at the time of manufacture raises concerns that all keys could be kept (perhaps surreptitiously) in some master databank that would be accessible without going to the designated escrow agents. The implication is that the user is forced to trust several organizations and

individuals involved with the manufacturing process. Such trust becomes an implicit aspect of the secrecy associated with EES-compliant devices.

One alternative to unit key generation at birth is the generation (or input) of a new unit key at user request. This approach has the advantage that the user can be confident that no one else retains a copy of the new key without his or her knowledge. The disadvantage is that escrow of that key would require explicit action on the user's part for that purpose.

An alternative that has some of the advantages of each approach is to install and register a unit key at birth, but to design the product to allow the user to change the unit key later. Thus, all products designed in this manner would have "default" unit keys installed by the manufacturer and recorded with some escrow agent; each of these keys would be different. Users who took the trouble to install a new unit key would have to take an explicit action to escrow it, but in many cases the inconvenience and bother of changing the unit key would result in no action being taken. Thus, valid unit keys would be held by escrow agents in two cases--for products owned by users who did not change the unit key, and for products owned by users who chose to register their new keys with escrow agents.

Who is responsible for the collection of unit keys? Under the Clipper/Capstone approach, the responsible party is the U.S. government. But if nongovernment agencies were to be responsible for escrowing keys (see Section 5.8), a large market with many vendors producing many different types of encryption products in large volume could result in a large administrative burden on these vendors.

The specific implementation of EES also raises an additional point. As proposed, EES requires that unit keys be given to government authorities upon presentation of legal authorization. If these keys are still available to the authorities after the period of legal authorization has expired, the EES device is forever open to government surveillance. To guard against this possibility, Administration plans for the final Clipper key escrow system provide for automatic key deletion from the decrypting equipment upon expiration of the authorized period. Key deletion is to be implemented on the tamper-resistant device that law enforcement authorities will use to decrypt Clipper-encrypted traffic. However, by early 1996, the

deployed interim key escrow system had not been upgraded to include that feature.

5.13 ISSUES RELATED TO THE ADMINISTRATION PROPOSAL TO relax export controls on 64-BIT ESCROWED ENCRYPTION IN SOFTWARE

As noted in Chapter 4, the Administration has proposed to treat software products with 64-bit encryption using any algorithm as it currently treats products that are based on 40-bit RC2/RC4 algorithms, providing that products using this stronger encryption are "properly escrowed." This change is intended to make available to foreign customers of U.S. software products stronger cryptographic protection than they currently have today. This proposal has raised several issues.

5.13.1 The Definition of "Proper Escrowing"

The definition of "proper escrowing" (as the phrase is used in the Administration's proposed new export rules in Box 5.3) is that keys should be escrowed only with "escrow agent(s) certified by the U.S. Government, or certified by foreign governments with which the U.S. Government has formal agreements consistent with U.S. law enforcement and national security requirements." These agents would not necessarily be government agencies, although in principle they could be.

The obvious question is whether foreign consumers will be willing to purchase U.S. products with encryption capabilities when it is openly announced that the information security of those products could be compromised by or with the assistance of escrow agents certified by the U.S. government. While the draft definition does envision the possibility that escrow agents could be certified by foreign governments (e.g., those in the country of sale), formal agreements often take a long time to negotiate, during which time U.S. escrow agents would hold the keys, or the market for such products would fail to develop.

For some applications (e.g., U.S. companies doing business with foreign suppliers), interim U.S. control of escrow agents may prove acceptable. But it is easy to imagine other applications for which it would not, and in any case a larger question is begged: What would be the incentive for foreign users to purchase such products from U.S. vendors if comparably strong but unescrowed foreign products with encryption capabilities were available? As the discussion

in Chapter 2 points out, integrated products with encryption capabilities are generally available today from U.S. vendors. However, how long the U.S. monopoly in this market will last is an open question.

The issue of who holds the keys in an international context is explored further in Appendix G.

5.13.2 The Proposed Limitation of Key Lengths to 64 Bits or Less

The most important question raised by the 64-bit limitation is this: If the keys are escrowed and available to law enforcement and national security authorities, why does it matter how long the keys are? In response to this question, senior Administration officials have said that the limitation to 64 bits is a way of hedging against the possibility of finding easily proliferated ways to break the escrow binding built into software, with the result that U.S. software products without effective key escrow would become available worldwide. Paraphrasing the remarks of a senior Administration official at the International Cryptography Institute 1995 conference, "The 64-bit limit is there because we might have a chance of dealing with a breakdown of software key escrow 10 to 15 years down the line; but if the key length implied a work factor of something like triple-DES, we would never [emphasis in original] be able to do it."

Two factors must be considered in this argument. One is the likelihood that software key escrow can in fact be compromised. This subject is considered in Sections 5.10.2 and 5.11. But a second point is the fact that the 64-bit limit is easily circumvented by multiple encryption under some circumstances. Specifically, consider a stand-alone security-specific product for file encryption that is based on DES and is escrowed. Such a product--in its unaltered state--meets all of the proposed draft criteria for export. But disassembly of the object code of the program (to defeat the escrow binding) may also reveal the code for DES encryption in the product. Once the source code for the DES encryption is available, it is a technically straightforward exercise to implement a package that will use the product to implement a triple-DES encryption on a file.

5.14 RECAP

Escrowed encryption is one of several approaches to

providing exceptional access to encrypted information. The U.S. government has advanced a number of initiatives to support the insertion of escrow features into products with encryption capabilities that will become available in the future, including the Escrowed Encryption Standard, the Capstone/Fortezza initiative, and a proposal to liberalize export controls on products using escrowed encryption. Its support of escrowed encryption embodies the government's belief that the benefit to law enforcement and national security from exceptional access to encrypted information outweighs the damage owing to loss of confidentiality that might occur with the failure of procedures intended to prevent unauthorized access to the escrow mechanism.

Escrowed encryption provides more confidentiality than leaving information unprotected (as most information is today), but less confidentiality than what could be provided by good implementations of unescrowed cryptography. On the other hand, escrowed encryption provides more capability for exceptional access under circumstances of key loss or unavailability than does unescrowed encryption. All users will have to address this trade-off between level of confidentiality and key unavailability.

The central questions with respect to escrowed encryption are the following:

- With what degree of confidence is it possible to ensure that third parties will have access to encrypted information only under lawfully authorized circumstances?
- What is the trade-off for the user between potentially lower levels of confidentiality and higher degrees of confidence that encrypted data will be available when necessary?

1See "Statement by the Press Secretary, The White House, April 16, 1993," reprinted in David Banisar (ed.), 1994 Cryptography and Privacy Sourcebook, Part II, Electronic Privacy Information Center, Diane Publishing, Upland, Pa., 1994. The name "Clipper" initially selected as the name of this effort proved later to be a trademark whose holder relinquished it to public use.

2In the more general meaning of escrowed encryption, exceptional access refers to access to plaintext by a party other than the originator and the recipient of encrypted communications. For the case of stored information,

exceptional access may refer to access to the plaintext of an encrypted file by someone not designated by the original encryptor of the file to decrypt it or even by persons so designated who have forgotten how to do so. See also Chapter 3.

3See, for example, statement of Raymond Kammer, Deputy Director, National Institute of Standards and Technology, before the Committee on the Judiciary, U.S. Senate, May 3, 1994. Available on-line at http://www.nist.gov/item/testimony/may94/encryp.html.

4Dorothy Denning and Miles Smid, "Key Escrowing Today," IEEE Communications, Volume 32(9), September 1994, pp. 58-68. Available on-line at http://www.cosc.georgetown.edu/~denning/crypto/Key-Escrowing-Today.txt.

5See Ernest Brickell et al., SKIPJACK Review: Interim Report, July 28, 1993. Posted to the "sci.crypt" newsgroup on August 1, 1993, by Dorothy Denning and available on-line at http://www.cosc.georgetown.edu/~denning/SKIPJACK.txt. Reprinted in Lance J. Hoffman (ed.), Building in Big Brother: The Cryptographic Policy Debate, Springer-Verlag, New York, 1995, pp. 119-130.

6The device key or unit key is used to open the encryption that protects a session key. Hence, possession of the unit key allows the decryption of all messages or files encrypted with that unit or device. "Session key" is defined in footnote 7.

7"Session," as in computer science, denotes a period of time during which one or more computer-based processes are operational and performing some function; typically two or more of systems, end users, or software processes are involved in a session. It is analogous to a meeting among these things. For cryptography, a session is the plaintext data stream on which the cryptographic process operates. The session key is the actual key that is needed to decrypt the resulting ciphertext. In the context of an encrypted data transmission or telephone call, the session key is the key needed to decrypt the communications stream. For encrypted data storage, it is the key needed to decrypt the file. Note that in the case of symmetric encryption (discussed in Chapter 2), the decryption key is identical to the encryption key. Since asymmetric encryption for confidentiality is efficient only for short messages or files, symmetric encryption is used for session encryption

of telephony, data transmissions, and data storage.

8Because the family key would be known to law enforcement officials, obtaining the unencrypted LEAF would present no problems.

9Questions have arisen about NSA access to escrowed keys. NSA has stated for the record to the committee that "key escrow does not affect either the authorities or restrictions applicable to NSA's signals intelligence activities. NSA's access to escrowed keys will be tied to collection against legitimate foreign intelligence targets. The key holder must have some assurance that NSA is involved in an authorized intelligence collection activity and that the collection activity will be conducted in accordance with the appropriate restrictions." For a description of these restrictions, see Appendix D of this report.

10Dorothy Denning and Miles Smid, "Key Escrowing Today," IEEE Communications, Volume 32(9), 1994, pp. 58-68. Available on-line at http://www.cosc.georgetown.edu/~denning/crypto/Key-Escrowing-Today.txt. Given its initial intent to preserve law enforcement's ability to conduct wire taps, it follows that Clipper key escrow would be conducted without the knowledge of parties whose keys had been escrowed, and would be conducted according to a set of rules that would be publicly known but not changeable by the affected parties. Under the requirements of Title III, the affected parties would be notified of the tapping activity at its conclusion, unless the information were to become the basis for a criminal indictment or an ongoing investigation. In the latter case, the accused would learn of the wiretaps, and hence the law enforcement use of escrowed keys, through court procedures.

11For example, an opinion issued by the Congressional Research Service argues that legislation would be required to mandate the use of the Clipper chip beyond federal computer systems. Memorandum from the American Law Division, Congressional Research Service, "Current Legal Authority to Mandate Adoption of ÔClipper Chip' Standards by Private Parties," Library of Congress, Washington, D.C., October 4, 1994.

12AT&T Secure Communications product literature, available on-line at http://www. att.com/press/0694/940613.pdb.html, and personal communication with Bruce Bailey, AT&T Secure

Communications Systems, Greensboro, N.C., March 29, 1996.

13AT&T news release, "AT&T, Cycomm International Develop Digital Voice Encryption," November 1, 1995. Available on-line at http://www.att.com/press/1195/951101. mma.html.

14Technically speaking, Clipper and Capstone/Fortezza are not separate initiatives. The Capstone program had been under way for a number of years prior to the public announcement of the Clipper chip in 1993, and the Clipper chip is based entirely on technology developed under the Capstone program. The Clipper chip was developed when the incoming Clinton Administration felt it had to address the problem of voice encryption. However, while Clipper and Capstone/Fortezza are not technically separate programs, the public debate has engaged Clipper to a much greater degree than it has Capstone. For this reason, this report discusses Clipper and Capstone/Fortezza separately.

15The Fortezza card was previously named the Tessera card; the name was changed when previous trademark claims on "Tessera" were discovered.

16To ensure that the holder of the Fortezza card is in fact the authorized holder, a personal identification number (PIN) is associated with the card: only when the proper PIN is entered will the Fortezza card activate its various functions. While concerns have been raised in the security literature that passwords and PINs are not secure when transmitted over open communications lines, the PIN used by the Fortezza card is never used outside the confines of the user's system. That is, the PIN is never transmitted over any network link; the sole function of the PIN is to turn on the Fortezza card, after which an automated protocol ensures secure authentication.

17For example, such devices are made by Cylink and Telequip. See Government Computer News, "Security Device Is 007 in Your Pocket," August 7, 1995, p. 6.

18Paul Constance, "DoD Plans to Install 750,000 Fortezza Cards," Government Computer News, July 31, 1995, p. 1 for the solicitation.

19For example, the Netscape Communications Corporation has announced that it will support Fortezza in the next version of its Web browser, while the Oracle Corporation will support Fortezza in the next version of its Secure Network

Services product. See Elizabeth Sikorovsky, "Netscape and Oracle Products Support Fortezza Card," Federal Computer Week, October 23, 1995, p. 36.

20See "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure," Executive Office of the President, Office of Management and Budget, Washington, D.C., May 20, 1996.

21An example first announced in 1994 is Northern Telecom's "Entrust," which provides for file encryption and digital signature in a corporate network environment using RSA public-key cryptography. "Entrust" allows master access by a network administrator to all users' encrypted files, even after a user has left the company. A product review for a recent version of "Entrust" can be found in Stephen Cobb, "Encryption for the Enterprise," Network World, March 11, 1996, p. 57.

22All of these examples are taken from Dorothy Denning and Dennis Branstad, "A Taxonomy of Key Escrow Encryption," Communications of the ACM, Volume 39, March 1996.

23This comment was probably made during the meetings of July, August, and September 1993 by the Computer System Security and Privacy Advisory Board to solicit public views on the Clipper initiative. Transcripts of the meetings are available from the National Institute of Standards and Technology.

24Stephen T. Walker et al., Commercial Key Escrow: Something for Everyone Now and for the Future, Report #541, Trusted Information Systems, Glenwood, Md., January 1995.

25Adi Shamir, "Partial Key Escrow: A New Approach to Software Key Escrow," summary of presentation at NIST FIPS Key Escrow Workshop, National Institute of Standards and Technology, Gaithersburg, Md., September 15, 1995. Available on-line at http://reality.sgi.com/employees/chrisr_corp/pkedc.html.

26Even worse, it is not just future communications that are placed at risk, but past communications as well. For example, if encrypted conversations are recorded and the relevant key is not available, they are useless. However, once the unit key is obtained, those recordings become decipherable if they are still available. Such recording would be illegal, because legal authorization for the

wiretap would have been necessary to obtain the key, but since these circumstances presume a breakdown of escrow procedures in the first place, the fact of illegality is not particularly relevant.

27For example, if a party external to the corporation has the keys that provide access to that corporation's encrypted information, the corporation is more vulnerable to a loss of confidentiality, because the external party can become the target of theft, extortion, blackmail, and the like by unauthorized parties who are seeking that information. Of course, the corporation itself is vulnerable, but since only one target (either the corporation or any external key-holding party) needs to be compromised, more targets lead to greater vulnerability. Of course, if keys are split among a number of external parties, the likelihood of compromise through this route is reduced, but the overall risk of compromise is still increased.

28See, for example, Peter G. Neumann, Computer-Related Risks, Addison-Wesley, New York, 1995; and Charles Perrow, Normal Accidents: Living with High-Risk Technologies, Basic Books, New York, 1984. Neumann describes a large number of computer-related reliability and safety problems and security vulnerabilities that have arisen from combinations of defective system implementation, flawed system design, and human error in executing procedures. Perrow describes a number of accidents that have occurred in other domains (e.g., maritime shipping, air traffic control, nuclear power plant operation) that have resulted from a similar set of problems.

29"Voluntary" has been used ambiguously in the public debate on key escrow. It can mean voluntary use of key escrow in any context or implementation, or it can mean voluntary use of EES-compliant products. In the latter situation, of course, the key-escrow feature would be automatic. Usually, the context of its use will clarify which interpretation of "voluntary" is intended.

30Cf. point in Chapter 2 regarding behavior of criminals with respect to wiretapped telephone calls.

31For example, at present the Department of Defense requires that contractors acquire and employ STU-III secure telephones for certain sensitive telephonic communications with DOD personnel. The Federal Acquisition Regulations (FAR) were modified to allow the costs of such telephones to

be charged against contracts, to further encourage purchase of these telephones.

32One major manufacturer noted to the committee that meeting federal requirements for encryption also reduces its ability to standardize on a single solution in distributed networks. Government-mandated key escrow could differ substantially enough from key escrow systems required for commercial operations that two separate key escrow systems could be needed.

33On July 20, 1994, Vice President Al Gore wrote to Representative Maria Cantwell (D-Washington) expressing a willingness to enter into "a new phase of cooperation among government, industry representatives and privacy advocates with a goal of trying to develop a key escrow encryption system that will provide strong encryption, be acceptable to computer users worldwide, and address our national security needs as well." The Vice President went on to say that "we welcome the opportunity to work with industry to design a more versatile, less expensive system. Such a key escrow system would be implementable in software, firmware, hardware, or any combination thereof, would not rely upon a classified algorithm, would be voluntary, and would be exportable. . . . We also recognize that a new key escrow encryption system must permit the use of private-sector key escrow agents as one option. . . . Having a number of escrow agents would give individuals and businesses more choices and flexibility in meeting their needs for secure communications." Letter reprinted in Hoffman, Building in Big Brother, 1995, pp. 236-238.

34The original Clipper/Capstone proposal made no provision for parties other than law enforcement authorities to approach escrow agents, and in this context could be regarded as a simple law enforcement initiative with no particular relevance to the private sector. However, in light of the Administration's arguments concerning the desirability of escrowed encryption to meet the key backup needs of the private sector, the importance of relevance to the private sector is obvious.

35For example, in the early days of an offering by AT&T to provide picture-phone meeting services, the question arose as to whether AT&T or the end user should provide security. The business decision at the time was that AT&T should not provide security because of the legal implications--a company that guaranteed security but failed to provide it

was liable. (Ironically, at least one major computer vendor declined to provide encryption services for data communications and storage on the grounds that encryption would be provided by AT&T.) While today's AT&T support for the PictureTel product line for videoconferencing (which provides encryption capabilities) may suggest a different AT&T perspective on the issue of who is responsible for providing security, companies will have to decide for themselves their own tolerable thresholds of risk for liability.

36The cost of vendor registration would be high in the case of certain software products. Specifically, products that are distributed by CD-ROM must be identical, because it would be very expensive (relative to current costs) to ship CD-ROMs with unique serial numbers or keys. To some extent, the same is true of products distributed by network--it is highly convenient and desirable from the vendor's perspective to have just one file that can be downloaded upon user request, although it is possible and more expensive to provide numbered copies of software distributed by network.

37Under a site license, a corporation agrees with a vendor on a price for a certain (perhaps variable) number of licenses to use a given software package. Site licenses also include agreements on and conditions for support and documentation.

38The dominance of corporate sales over sales to individuals was cited in Department of Commerce and National Security Agency, A Study of the International Market for Computer Software with Encryption, released January 11, 1996, p. III-2.

39Note also that maintaining the physical security of escrow agents, especially government escrow agents, may be especially critical; sabotage or destruction of an escrow agent facility might well be seen in some segments of society as a blow for freedom and liberty.

40A similar issue arises with respect to certificate authorities for authentication. As discussed in Chapter 2, a cryptography-based authentication of an individual's identity depends on the existence of an entity--a certification authority--that is trusted by third parties as being able to truly certify the identity of the individual in question. Concentration of certification authority into

a single entity would imply that an individual would be vulnerable to any penetration or malfeasance of the entity and thus to all of the catastrophic effects that tampering with an individual's digital identity would imply.

41Nothing in this discussion is intended to preclude the possibility that an organization serving as an escrow agent might also have responsibilities as a certification authority (for authentication purposes, as described in Chapter 2).

42See, for example, Silvio Micali, "Fair Public-Key Cryptosystems," in Advances in Cryptology--Crypto Ô92, Springer-Verlag, Heidelberg, 1993, pp. 113-138.

43See, for example, Computer Science and Telecommunications Board, National Research Council, Computers at Risk: Safe Computing in the Information Age, National Academy Press, Washington, D.C., 1991.

44U.S. Department of Justice, Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title III and FISA, February 4, 1994. Reprinted in Hoffman (ed.), Building in Big Brother, 1995, pp. 243-246.

45Even if these transactions are authenticated (as most large transactions would be), large transactions that are compromised could lead to loss of bids and the like by the firms involved in the transaction.

46A kind of de facto secret back door can result from the fact that vendors of security products employing Clipper or Capstone technology are not likely to advertise the fact that the relevant encryption keys are escrowed with the U.S. government. Thus, even if the escrowing capability is "open" in the sense that no one involved makes any attempt to hide that fact, a user that does not know enough to ask about the presence or absence of escrowing features may well purchase such products without realizing their presence. Functionally, escrowing of which the user is ignorant is equivalent for that user to a "secret" back door.

47Of course, if other strong algorithms are known publicly, the force of this argument is weakened from a practical standpoint. For example, it is not clear that the disclosure of Skipjack would be harmful from the standpoint of making strong algorithms public, because triple-DES is

already publicly known, and triple-DES is quite strong.

48As one example, the RC2 encryption algorithm, nominally a trade secret owned by RSA Data Security Inc. was posted to the Internet in early 1996, apparently as the result of an apparent "disassembly" of a product embedding that algorithm (personal communication, Robert Baldwin, RSA Data Security Inc., May 16, 1996).

49For example, Trusted Information Systems Inc. of Glenwood, Md., has advocated an approach to preventing modification that relies on the placement of integrity checks at strategic locations. With such an approach, a change to the disassembled source code would have to be reflected properly in all relevant integrity checks; doing so might well involve disassembly of an entire product rather than of just one module of the product. Nevertheless, such an approach cannot prevent modification, although it can make modification more difficult. Such anti-reverse-engineering features may also increase the difficulty of vendor maintenance of a product. Increased difficulty may be a price vendors must pay in order to have more secure software implementations.

50Estimates of the cost to reverse-engineer the Clipper chip nondestructively cover a wide range, from "doable in university laboratories with bright graduate students and traditions of reverse engineering" (as estimated by a number of electrical engineers in academia with extensive experience in reverse engineering) to as much as $30 million to $50 million (as estimated in informal conversations between JASON members and DOD engineers). The cost may well be lower if large numbers of chips are available for destructive inspection.

51According to Dorothy Denning, the review team for Skipjack (see footnote 5 of this chapter) compared the output from Clipper chips with output from the software version of Skipjack that the review team obtained for review to verify that the algorithm on the chips was the same as the software version (personal communication, Dorothy Denning, Georgetown University, March 1996).

52As described in Chapter 4, the product tester can use the product to encrypt a randomly chosen set of values with a randomly chosen key, and compare the encrypted output to the known correct result obtained through the use of a product known to implement the algorithm correctly. This is known

as a vector test.

53Such a comment is not meant to preclude the possibility of an independent certifying authority, a kind of "Consumers' Union" for cryptography equipment and products. Such organizations have been proposed to evaluate and certify computer security, and as of this writing, three U.S. firm have received NIST approval to evaluate the conformance of products to FIPS 140-1, the FIPS for cryptography modules.

54This security problem is referenced in footnote 34, Chapter 2. The lack of prior vetting for Netscape Navigator is described by Kathleen Murphy, "A Second Security Breach," Web Week, Volume 1(6), October 1995, p. 8.

55In a recent contract, a vendor agreed to provide Fortezza cards at $69 per card. See Paul Constance, "After Complaining $99 Was Too Low, Fortezza Vendors Come in at $69," Government Computer News, October 2, 1995, p. 6.

56 One vendor is manufacturing a circuit board for encryption that fits into a 3.5" floppy disk drive. However, this device does not employ the Capstone/Foretzza approach. See Elizabeth Sikorovsky, "Device Offers Alternative to PC Card-Based Encryption," Federal Computer Week, November 13, 1995, pp. 29 and 35.

57Note that the dividing line between hardware and software is not always clear. In particular, product designers use the term "firmware" to refer to a design approach that enters software into a special computer memory (an integrated circuit chip) that usually is subsequently unchangeable (read-only memory; ROM). Sometimes an alternate form of memory is used that does permit changes under controlled conditions (electrically programmable ROM; EPROM). Such software-controlled hardware (microprogrammed hardware) has the convenience that the functionality of the item can be updated or changed without redesign of the hardware portion.

58Peter G. Neumann, Can Systems Be Trustworthy with Software-Implemented Cryptography?, SRI International, Menlo Park, Calif., October 28, 1994.

59A device controlled by software stored in read-only memory is for all intents and purposes the same as "pure hardware" in this context.

60A Clipper chip costs about $10 when bought in large lots (personal communication, Jimmy Dolphin, Mykotronx, March 22, 1996). Even when including retail mark-up costs and labor, the cost of changing a Clipper chip is likely to be less than $100.

61However, since the Skipjack algorithm is classified, simple knowledge of the unit key (or the session key) would enable only those with knowledge of the algorithm to decrypt the session key (or the session).